SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

HEARING

BEFORE THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

FIRST SESSION

MARCH 1, 2017

Serial No. 115–2

Printed for the use of the Committee on the Judiciary

Available via the World Wide Web: http://judiciary.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE

24–726 PDF WASHINGTON : 2017

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

BOB GOODLATTE, Virginia, *Chairman*

F. JAMES SENSENBRENNER, JR., Wisconsin
LAMAR S. SMITH, Texas
STEVE CHABOT, Ohio
DARRELL E. ISSA, California
STEVE KING, Iowa
TRENT FRANKS, Arizona
LOUIE GOHMERT, Texas
JIM JORDAN, Ohio
TED POE, Texas
JASON CHAFFETZ, Utah
TOM MARINO, Pennsylvania
TREY GOWDY, South Carolina
RAÚL LABRADOR, Idaho
BLAKE FARENTHOLD, Texas
DOUG COLLINS, Georgia
RON DeSANTIS, Florida
KEN BUCK, Colorado
JOHN RATCLIFFE, Texas
MARTHA ROBY, Alabama
MATT GAETZ, Florida
MIKE JOHNSON, Louisiana
ANDY BIGGS, Arizona

JOHN CONYERS, JR., Michigan, *Ranking Member*
JERROLD NADLER, New York
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
STEVE COHEN, Tennessee
HENRY C. "HANK" JOHNSON, JR., Georgia
TED DEUTCH, Florida
LUIS V. GUTIERREZ, Illinois
KAREN BASS, California
CEDRIC RICHMOND, Louisiana
HAKEEM JEFFRIES, New York
DAVID N. CICILLINE, Rhode Island
ERIC SWALWELL, California
TED LIEU, California
JAMIE RASKIN, Maryland
PRAMILA JAYAPAL, Washington
BRADLEY SCHNEIDER, Illinois

SHELLEY HUSBAND, *Chief of Staff & General Counsel*
PERRY APELBAUM, *Minority Staff Director & Chief Counsel*

CONTENTS

MARCH 1, 2017

SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

WEDNESDAY, MARCH 1, 2017

HOUSE OF REPRESENTATIVES
COMMITTEE ON THE JUDICIARY
Washington, DC.

The Committee met, pursuant to call, at 1:36 p.m., in room 2141, Rayburn House Office Building, the Honorable Bob Goodlatte (Chairman of the Committee) presiding.

Present: Representatives Goodlatte, Jordan, Poe, Marino, Labrador, Conyers, and Lieu.

Staff Present: (Majority) Shelley Husband, Chief of Staff & General Counsel; Branden Ritchie, Deputy Chief of Staff & Chief Counsel; Zach Somers, Parliamentarian and General Counsel; Ryan Breitenbach, Counsel, Subcommittee on Crime, Terrorism, Homeland Security, and Investigations; (Minority) Joe Graupensperger, Chief Counsel, Subcommittee on Crime, Terrorism, Homeland Security, and Investigations; and Veronica Eligan, Professional Staff Member.

Mr. GOODLATTE. The Committee will reconvene. Today's unclassified hearing follows a classified panel in which Members of the Judiciary Committee heard testimony from the Federal Bureau of Investigation, National Security Agency, Department of Justice, and the Office of the Director of National Intelligence regarding the operations and constitutionality of Section 702 of the Foreign Intelligence Surveillance Act, or FISA.

In February 2016, the Judiciary Committee held a classified hearing that began our consideration of the reauthorization of the FISA Amendments Act, which was first signed into law in 2008 and reauthorized in 2012.

Our hearing last year served as a good background and foundational update on the status of national security operations under the law. Much has happened since the law was last reauthorized, however, including the unauthorized disclosures of classified information by Edward Snowden in 2013 that spawned significant public debate on U.S. Government surveillance.

We also have many new Members who have not yet had an opportunity to directly question experts regarding the statute's successes or areas where reform may be needed.

Finally, we have very recent jurisprudence upholding the statute's constitutionality. Like congressional oversight, judicial oversight of this program is an integral safeguard, so exploring various

courts' legal analysis concerning 702 will be beneficial for our own oversight as well.

Congress enacted FISA in 1978 to establish statutory guidelines authorizing the use of electronic surveillance in the United States for foreign intelligence purposes. Following enactment, global communications infrastructure shifted from satellite to fiberoptic wire, altering the manner in which domestic and foreign communications are transmitted.

This technological shift had the adverse and unintended effect of requiring the government to obtain an individualized FISA court order to monitor foreign communications by non-U.S. persons. The government had to obtain probable cause to investigate a foreign national located overseas, an untenable proposition that served to extend rights under the U.S. Constitution extraterritorially and limit lawful U.S. intelligence activities.

In 2008, the FISA Amendments Act corrected this anomaly by establishing procedures for the collection of foreign intelligence on targets located outside U.S. borders. At its core, Section 702 of the act permits the attorney general and the director of national intelligence to jointly authorize the targeting of non-U.S. persons reasonably believed to be located outside the United States.

As an important safeguard, the act prohibits the use of Section 702 to intentionally target a person inside the United States and forbids so-called reverse targeting using Section 702 to target a person outside this country if the true purpose of the acquisition is to target someone inside the United States.

Furthermore, the government may not acquire a communication to which all parties are known to be inside the U.S., and all Section 702 acquisitions must be conducted in a manner consistent with the Fourth Amendment to the Constitution of the United States.

Section 702 also prohibits the intentional targeting of a U.S. person outside the United States. Instead, Sections 703 and 704 of the act preserve Fourth Amendment protections for U.S. citizens by requiring the government to obtain an individualized order from the FISA court, known as the FISC, to acquire U.S. persons' communications while they are outside the United States.

America's intelligence community has deemed Section 702 its most important tool in battling terrorism. However, it has also been criticized by some as an overly broad program that collects communications of U.S. citizens without sufficient legal process. Today's classified and public panels afford Members an opportunity to examine Section 702 collection in greater detail and probe the aspects of this important collection with which they may be concerned.

The Judiciary Committee has primary jurisdiction over FISA. During Committee consideration of the USA FREEDOM Act, I made a commitment to Members that the Committee would separately undertake fulsome oversight of the FISA Amendments Act, which is slated to expire on December 31 of this year. This hearing is the first step of this Congress toward a detailed, thorough, and careful examination.

I thank all of our witnesses for testifying today. These individuals represent multiple viewpoints to ensure that this is a well-rounded debate that gives voice to diverse stakeholders. We must

ensure that our protection doesn't come at the expense of cherished liberty.

Every single one of us who has promised to uphold the Constitution has a duty to ensure that surveillance authorities are crafted and employed in a manner consistent with our oath and the expectation of all Americans. Strong and effective national security tools, like Section 702, and civil liberties can and must coexist.

With that, I am pleased to welcome and recognize the Ranking Member of the Committee, the gentleman from Michigan, Mr. Conyers, for his opening statement.

Mr. CONYERS. Thank you, Chairman Goodlatte.

And I thank the second panel of witnesses for being here and joining us today.

As has been noted, last Congress we enjoyed a relative amount of success working together in a bipartisan fashion to pass the USA FREEDOM Act. We demonstrated that privacy and security are not necessarily mutually exclusive values.

Our bill did not contain every reform I had hoped to see, but it shows that our Committee is capable of crafting authorities that serve the government's needs and respects our commitment to civil liberties. There are a few important lessons from that project worth repeating as we undertake this next round of surveillance reform.

We're all in this together. The Members of the Committee include some of the most progressive Democrats and conservative Republicans in the Congress, but no matter. We have shown that both in this Committee and on the House floor we can build consensus around our common values. Among those values are a dedication to privacy, to transparency in government, and to the protection from unreasonable search guaranteed to the people by the Fourth Amendment.

I've enjoyed working with our coalition in the past, and I look forward to doing so here as we seek the basic reform that I think is needed for Section 702.

We cannot do this work well without the assistance of the intelligence community. On April 22, 2016, several Members of this Committee wrote to Director Clapper to request that he prepare a public estimate of the impact of Section 702 on United States citizens. We were not the first to make this request. As early as 2011, Senator Wyden and Senator Udall had asked for similar information.

By the time we wrote our letter, more than 30 civil liberties organizations had petitioned the director for the same. I was encouraged by the government's initial response. ODNI and NSA took the extraordinary step of holding an unclassified briefing for our personal staffs. Over the next few months, they held additional discussion with Committee counsel. On December 16, our group of Members again wrote to Director Clapper to memorialize our understanding of the project.

The government has pledged to provide us with an estimate of the impact of 702 on United States citizens. Both the estimate and the methodology used to reach it will be made public. The government also promised to provide this information in time to inform the debate on reauthorization when it begins.

And without objection, I ask that both letters of mine be placed in the record.*

Mr. GOODLATTE. Without objection, they will be made a part of the record.

Mr. CONYERS. Thank you.

Unfortunately, here we are at the beginning of our debate and the intelligence community has not so much as responded to our December letter, let alone completed the project. I had hoped for better.

The Members of this Committee and the public at large require that estimate if we're to engage in a meaningful debate. We'll not simply take the government's word on the size of the so-called incidental collection.

And this problem illustrates my final observation: We should all do a better job of distinguishing between technical legal arguments and the values at play in this discussion. They're both different, and they're both important.

Here are the facts. The law prohibits the government from using Section 702 to target any United States citizen. Nevertheless, the government can and does collect massive amounts of information about our citizens under this authority. The Members here are well aware that this practice has been read into the statute by the government and ratified many times over by the Foreign Intelligence Surveillance Court.

We know it is not unlawful in that respect. We also understand that the men and women of the intelligence community have a duty to keep us safe within the four corners of the law and that they take this obligation seriously.

Our criticism comes from someplace else. The idea of using this authority to collect large amounts of information about United States citizens without a warrant or individualized suspicion and then applying that information to purposes having nothing to do with counterintelligence or counterterrorism is, in a word, wrong. It does not comport with our values or those that underscore the Fourth Amendment to the Constitution.

And at the end of the day, as the sunset of this authority draws near, the manner in which one collects, retains, and disseminates this information is only lawful if Congress says it is. And so I am eager to hear those witnesses that are present with us today and engage in this inquiry.

I thank the Chairman and yield back any time remaining.

Mr. GOODLATTE. The Chair thanks the gentleman.

We would welcome our distinguished witnesses today. And if you would all please rise, I'll begin by swearing you in.

Do you and each of you solemnly swear that the testimony you are about to give shall be the truth, the whole truth, and nothing but the truth, so help you God?

Thank you.

Let the record reflect that all the witnesses have responded in the affirmative.

***Note:** The submitted material is not printed in this hearing record but is on file with the Committee, and can also be accessed at:

http://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=105619

Mr. Jeff Kosseff is the assistant professor of the United States Naval Academy's Cyber Science Department. Previously, Professor Kosseff practiced cybersecurity and privacy law at Covington & Burling and clerked for Judge Milan D. Smith, Jr., of the United States Court of Appeals for the Ninth Circuit, and for Leonie M. Brinkema of the United States District Court for the Eastern District of Virginia.

Before becoming a lawyer, he was a journalist for the Oregonian and was a finalist for the Pulitzer Prize for national reporting and recipient of the George Polk Award. He is a graduate of Georgetown University Law Center and the University of Michigan.

April Doss is currently a partner at the law firm Saul Ewing, where she chairs the firm's Cybersecurity and Privacy Practice Group. From 2003 to 2016, Ms. Doss worked at the National Security Agency where she served in a variety of roles. She worked on information-sharing policy, managed counterterrorism programs, led innovative compliance processes in new technology development, served as an intelligence oversight program manager, lived overseas as a foreign liaison officer, and provided legal advice on NSA's intelligence activities.

From 2014 to 2016, she was the associate general counsel for intelligence law responsible for providing legal advice on NSA's global intelligence operations, technology capabilities, privacy and civil liberties, and oversight and compliance programs. Ms. Doss is a graduate of Goucher College, Yale University, and UC Berkeley Law.

Elizabeth Goitein co-directs the Brennan Center for Justices' Liberty and National Security Program at the New York University School of Law. Before joining the Brennan Center, she served as counsel to U.S. Senator Russell Feingold. As counsel to Senator Feingold, Ms. Goitein handled a variety of liberty and national security matters with a particular focus on government secrecy and privacy rights.

Previously, she was a trial attorney in the Federal Programs Branch of the Civil Division of the Department of Justice. Ms. Goitein is a graduate of Yale University, the Juilliard School, and Yale Law School.

Adam Klein. Mr. Klein is a senior fellow at the Center for a New American Security, a bipartisan national security research organization in Washington. His research centers on the intersection of national security policy and law, including government surveillance in the digital age, counterterrorism, and rules governing the use of military force.

Previously, Adam served as a law clerk to Justice Antonin Scalia of the United States Supreme Court and Judge Brett Kavanaugh of the U.S. Court of Appeals for the D.C. Circuit, and was a senior associate at WilmerHale. He has also worked on national security policy at the Rand Corporation and the 9/11 Public Discourse Project. He is a graduate of Northwestern University and Columbia Law School.

Welcome to all of you. We will proceed under the 5-minute rule. There is a timer, I think, right in front of you there. When you get down to 1 minute, I think it will warn you that you have 1 minute

left. Please summarize at that point. Your entire statement, written statement, will be made part of the record.

We'll start with you, Mr. Kosseff. Am I pronouncing your name correctly?

Mr. KOSSEFF. Yes.

Mr. GOODLATTE. Good.

TESTIMONY OF JEFF KOSSEFF, ASSISTANT PROFESSOR, CYBER SCIENCE DEPARTMENT, UNITED STATES NAVAL ACADEMY

Mr. KOSSEFF. Mr. Chairman, Mr. Ranking Member, and Members of the Committee, thank you for the opportunity to testify about 702. My name is Jeff Kosseff, and I'm an assistant professor at the U.S. Naval Academy, where I teach cybersecurity law. The views that I express today are only my own and do not necessarily represent the DOD or its components.

Some of my testimony today is drawn from a Hoover Institution paper that I published last year with my colleague, Chris Inglis, who served as the deputy director of the NSA. I initially was quite hesitant to work on a paper about 702 with the NSA's former deputy director. As a lawyer, I have represented media organizations sometimes adverse to government agencies.

Before becoming a lawyer, I was a journalist. I suspect the Committee would agree with me that journalists may be an especially skeptical bunch, and I was highly skeptical about the constitutionality of a government surveillance program that I understood primarily through reading the media accounts of the Snowden leaks.

Nonetheless, I evaluated the entirety of the program based not only on media reports, but also on the public primary source record. What I found was an effective program that is subject to rigorous oversight by the three branches of government and on balance complies with the Fourth Amendment.

That is not to say that I easily arrived at my conclusion, nor do I deny that there are some aspects of the program that raise very, very difficult Fourth Amendment questions.

To start with the Fourth Amendment analysis, we have to look at whether there was a warrant or an exception to the warrant requirement. I agree with the FISA Court of Review that foreign intelligence can be considered a special need that is separate from law enforcement and is exempt from the warrant requirement.

The FISA court has held that this exception covers 702, and I agree with this conclusion for the reasons stated in my written testimony. Even if warrants are not required, the Fourth Amendment demands an assessment of the reasonableness of the search by balancing the intrusion on individual privacy with the promotion of legitimate government interests.

The public record strongly supports the conclusion that 702 is an effective national security program. For example, the Privacy and Civil Liberties Oversight Board noted that more than 25 percent of the NSA's reports about international terrorism rely at least in part on 702 information. 702 is simply a more nimble alternative to Title I of FISA, which was designed to protect subjects who are U.S. persons.

On the other side of the balancing test, we must assess the invasion of the individual's privacy interests. The statute explicitly prohibits the government from using 702 to intentionally target persons known to be in the U.S. or U.S. persons, and it explicitly prohibits reverse targeting.

702 programs are subject to a number of additional procedural safeguards, including oversight from all three branches of government, certification requirements, and minimization and targeting procedures.

That said, the FBI's querying of 702 data for evidence of a crime, I believe, raises the most difficult Fourth Amendment issues. In a recent FISA court proceeding, amicus argued that each FBI query of 702 information is a separate action subject to the Fourth Amendment reasonableness test. Judge Hogan correctly rejected that formulation and instead evaluated the 702 program as a whole.

Judge Hogan set forth a compelling case as to why national security interests outweigh the intrusion on privacy. Importantly, the FBI and other agencies can only query data that has been obtained through the certification targeting and tasking procedures. Only a subset of the 702 information is available to the FBI for queries, and the FBI does not receive unminimized information obtained through the NSA's upstream process.

On balance, the FBI's ability to query 702 data as described in the public record does not render 702 unconstitutional. During the reauthorization process, Congress may well conclude that there are legitimate policy reasons to limit the FBI's ability to conduct such queries. However, my testimony today is limited to the application of the Fourth Amendment to 702.

The intelligence community continues to increase the amount of information available to the public about 702, and this is absolutely crucial. I commend these transparency efforts recognizing the tremendous difficulty caused by the inherently classified nature of foreign intelligence programs.

Further, and importantly, the work of the Privacy and Civil Liberties Oversight Board has been absolutely essential in informing the public debate about 702. The Fourth Amendment, like other important constitutional rights, is highly fact dependent, requiring close analysis of not only how the program is structured by statute, but how it actually is being implemented. And that analysis must be ongoing, and that's why transparency is so vital to our constitutional analysis.

Thank you, and I look forward to your questions.

[The testimony of Mr. Kosseff follows:]

TESTIMONY OF JEFF KOSSEFF

ASSISTANT PROFESSOR, CYBER SCIENCE DEPARTMENT

UNITED STATES NAVAL ACADEMY

BEFORE THE UNITED STATES HOUSE OF REPRESENTATIVES
JUDICIARY COMMITTEE

"SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT"

MARCH 1, 2017

Mr. Chairman, Mr. Ranking Member, and Members of the Committee, thank you for the opportunity to testify about Section 702 of the FISA Amendments Act.

My name is Jeff Kosseff, and I am an assistant professor in the United States Naval Academy's Cyber Science Department, where I teach cybersecurity law and policy. The views that I express at today's hearing are only my own, and do not necessarily represent the Naval Academy, Department of Navy, or Department of Defense. Additionally, I will note that my views are limited to the constitutionality of Section 702 as stated in the statute and explained in the public record; I have not worked in the intelligence community and therefore have no additional operational knowledge about the implementation of Section 702.

Some of my testimony today is drawn from a Hoover Institution paper[1] that I published last year with my colleague in the Naval Academy's Cyber Science Department, Chris Inglis, who served as the deputy director of the National Security Agency from 2006 to 2014.

I initially was hesitant to work on a paper about Section 702 of the FISA Amendments Act with the former head civilian executive of the NSA. As a lawyer, I have represented media organizations that were sometimes adverse to government agencies. Before becoming a lawyer, I was a journalist for more than seven years. I suspect the Committee would agree that journalists are an especially skeptical bunch, and that trait has stuck with me. I was highly skeptical about the constitutionality of a government surveillance program that I understood primarily through reading the media accounts of the Edward Snowden leaks, in which it initially was reported that the NSA and FBI "are tapping directly into the central servers of nine leading U.S. Internet companies, extracting audio, video, photographs, e-mails, documents, and connection logs that enable analysts to track a person's movements and contacts over time."[2]

Nonetheless, I evaluated the entirety of the program, based not only on media reports but also on the public primary source record. I examined publicly available information, including documents produced by the intelligence community, Foreign Intelligence Surveillance Court opinions, Congressional testimony, and the remarkably thorough report on Section 702 written by the Privacy and Civil Liberties Oversight Board (PCLOB).[3] As I will explain further, despite my initial skepticism, I found a program that is substantially different from the massive dragnet operation portrayed in the media reports. I discovered an effective foreign intelligence program that is subject to rigorous oversight by the three branches of government and, under the totality of the circumstances, complies with the Fourth Amendment.

---

[1] Chris Inglis & Jeff Kosseff, IN DEFENSE OF FAA SECTION 702: AN EXAMINATION OF ITS JUSTIFICATION, OPERATIONAL EMPLOYMENT, AND LEGAL UNDERPINNINGS (Hoover Institution) (2016) (hereinafter, "Hoover Paper").

[2] Barton Gellman, *U.S. Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST (June 6, 2013) (later revised) (as quoted by Peter Swire, U.S. SURVEILLANCE LAW, SAFE HARBOR, AND REFORMS SINCE 2013, white paper submitted to Belgian Privacy Forum (Dec. 17, 2015) at 14.

[3] Privacy and Civil Liberties Oversight Board, REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (July 2, 2014) (hereinafter, "PCLOB Report").

That is not to say that I easily arrived at my conclusion regarding the constitutionality of Section 702. Nor do I deny that there are some aspects of the program that raise difficult and close Fourth Amendment questions. Whenever there is the possibility of U.S. persons' communications being seized or searched by the government, the Fourth Amendment demands serious examination of the relevant privacy implications and safeguards.

For that reason, I will spend the remainder of my testimony explaining the principal factors that led to my conclusion that Section 702 comports with the Fourth Amendment. To do so, we look at the primary requirements of the Fourth Amendment: warrants supported by probable cause and reasonableness.

Fourth Amendment Warrant Requirement

Section 702 operates without court-issued warrants. The Supreme Court long has held that a search is exempt from the Fourth Amendment's warrant requirement "when special needs, beyond the normal need for law enforcement, makes the warrant and probable cause requirement impracticable."[4] Under this "special needs" exception, for instance, schools can conduct warrantless, random drug testing of school athletes.[5]

The U.S. Supreme Court never has directly decided whether foreign intelligence surveillance falls under the "special needs" exception to the warrant requirement.[6] However, the Foreign Intelligence Surveillance Court of Review has determined that foreign intelligence is a special need that is exempt from the warrant requirement in part because the purpose of foreign intelligence gathering "goes well beyond any garden-variety law enforcement objective."[7] The Foreign Intelligence Surveillance Court has concluded the foreign intelligence exception applies to Section 702, even though the program may result in the collection of communications of or concerning U.S. persons.[8] In reaching that conclusion, the Court emphasized that the national

---

[4] Griffin v. Wisconsin, 483 U.S. 868, 873 (1987) (internal quotation omitted).

[5] Vernonia School District 47J v. Acton, 515 U.S. 646, 653 (1995) ("We have found such 'special needs' to exist in the public school context. There, the warrant requirement 'would unduly interfere with the maintenance of the swift and informal disciplinary procedures [that are] needed,' and 'strict adherence to the requirement that searches be based on probable cause' would undercut 'the substantial need of teachers and administrators for freedom to maintain order in the schools.'") (quoting New Jersey v. T.L.O., 469 U.S. 325, 341 (1985)); *but see* Ferguson v. City of Charleston, 532 U.S. 67, 80–82 (2001) (refusing to find a special needs exception for a state hospital's involuntary drug testing of patients when "the central and indispensable feature of the policy from its inception was the use of law enforcement to coerce the patients into substance abuse treatment.").

[6] The Supreme Court stated in United States v. United States District Court (the Keith case), 407 U.S. 297 (1972) that surveillance for *domestic* security purposes requires a warrant, but explicitly left open the question of whether a warrant is required for foreign national security threats. *Id.* at 308-09, n.8, 321-22, n.20.

[7] In Re Directives, 551 F.3d 1004, 1011 (Foreign Intelligence Surveillance Court of Review 2008).

[8] *See* [Redacted Case Name], Memorandum Opinion, United States Foreign Intelligence Surveillance Court (Bates, J.) (Oct. 3, 2011) at 68.

security purpose of Section 702 collection not only well-exceeded ordinary law enforcement objectives, but also that there was a "high degree of probability that requiring a warrant" would impede the government's ability to "collect time-sensitive information" and cause harm to "vital national security interests."[9]

Accordingly, because foreign intelligence is a special need that is distinct from normal law enforcement, the Fourth Amendment does not require a warrant for Section 702.

Fourth Amendment Reasonableness

The Fourth Amendment inquiry, however, does not end upon determination that an exception to the warrant requirement applies. Even in cases in which warrants are not required, the Fourth Amendment requires an examination of the reasonableness of the search or seizure.[10] To assess reasonableness under the Fourth Amendment, courts weigh the "totality of the circumstances" of a search, balancing "on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate government interests."[11]

Government Interests

The public record strongly supports the conclusion that Section 702 is an effective national security program. The NSA stated that Section 702 collection "is the most significant tool in the NSA collection arsenal for the detection, identification, and disruption of terrorist threats to the U.S. and around the world."[12]

One challenge in conducting a public-facing analysis of a classified program is the lack of unclassified information about the program's benefits. Yet, even the relatively limited amount of information that the intelligence community has publicly provided makes clear that Section 702 serves a significant public benefit. Indeed, even critics of the program rarely dispute its effectiveness.

Section 702 is key to the extraordinarily difficult task of foreign intelligence surveillance. As PCLOB observed, "the hostile activities of terrorist organizations and other foreign entities are prone to being geographically dispersed, long-term in their planning, conducted in foreign languages or in code, and coordinated in large part from locations outside the reach of the United

---

[9] *Id.* at 69 (internal quotation marks and citations omitted).
[10] *See* Maryland v. King, 133 S.Ct. 1958, 1970 (2013) ("Even if a warrant is not required, a search is not beyond Fourth Amendment scrutiny; for it must be reasonable in its scope and manner of execution."); In Re Directives, 551 F.3d at 1012 ("[E]ven though the foreign intelligence exception applies in a given case, governmental action intruding on individual privacy interests must comport with the Fourth Amendment's reasonableness requirement.").
[11] Wyoming v. Houghton, 526 U.S. 295, 300 (1999).
[12] National Security Agency, THE NATIONAL SECURITY AGENCY: MISSIONS, AUTHORITIES, OVERSIGHT, AND PARTNERSHIPS (Aug. 9, 2013).

States."[13] Section 702 provides a valuable tool for the U.S. government to collect foreign intelligence information that traverses communications infrastructure in the United States.

To understand the operational benefits of Section 702, it is helpful to consider the primary alternative method to the program: obtaining a Foreign Intelligence Surveillance Court order under Title I of FISA. Because Title I was designed to protect subjects who are U.S. persons, the government must demonstrate probable cause to believe that "the target of the electronic surveillance is a foreign power or an agent of a foreign power[.]"[14] As Matthew G. Olsen, former director of the National Counterterrorism Center, testified before Congress last year, due to the growing number of foreign intelligence targets located overseas, "it was not practical to obtain individualized court orders on a routine basis."[15] Moreover, individuals are increasingly likely to have multiple email addresses and phone numbers, and are known to engage in the practice of changing them frequently, making it difficult to obtain individualized approval for each "selector."[16] Simply put, Section 702 is more nimble and better suited to modern communications infrastructure, when the communications of non-U.S. persons who are located outside of the United States may pass through the United States.[17]

After its careful review of Section 702, PCLOB concluded that the statute "has led the government to identify previously unknown individuals who are involved in international terrorism[,]"[18] and that, as of the time of the PCLOB report's drafting, more than 25 percent of NSA's reports about international terrorism relied at least in part on information gathered under Section 702.[19]

The concrete benefits of Section 702 are evident in the few declassified examples of how the government has used Section 702 data. For instance, the government used Section 702 information to arrest a man who had planned to attack a Danish newspaper that had printed cartoons of the Prophet Muhammad.[20] As a recent Heritage Foundation report summarized, "the fact remains that current and former intelligence officials, members from both political parties across two Administrations, national security law experts in the private sector, and the PCLOB

---

[13] PCLOB Report at 92.
[14] 50 U.S.C. § 1805(a)(2)(A).
[15] Testimony of Matthew G. Olsen, Hearing before the Senate Committee on the Judiciary (May 10, 2016) at 7.
[16] *See* Hoover Paper at 5 ("[I]t introduced a significant challenge for intelligence services which, under FISA 1978, had to obtain explicit approval for each and every selector they wanted to target. In 2008, there was a growing body of evidence that terrorists were making effective use of this agility, acquiring and shedding e-mail addresses and telephone numbers faster than US intelligence services could prepare, submit, and obtain required selector-by-selector approval.").
[17] *Id.* (describing "the transformation of technology between 1978 and 2008 during which time the vast portion of international communications (between nations) made a dramatic shift to physical cables (especially high-speed fiber optic cables) and domestic communications made increasing use of wireless modes of transmission.").
[18] PCLOB Report at 108.
[19] *Id.* at 10.
[20] House Committee on Intelligence, FOUR DECLASSIFIED EXAMPLES FROM THE NSA; *available at* http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/50attacks.pdf.

maintain that 702 has been and continues to be a very important intelligence tool for overseas intelligence collection."[21]

In short, even based on the limited amount of information in the public record, it is clear that Section 702 serves a vital national security interest. As an outside observer and academic, I urge the intelligence community to work to declassify additional examples of the practical use of Section 702 so that the general public can better understand the role that the program plays in national security.

Invasion of Privacy Interests

Having examined the government's interest, we must turn to the other side of the Fourth Amendment balancing test and assess the invasion of individual privacy interests. I agree with the growing consensus that individuals enjoy a Fourth Amendment reasonable expectation of privacy in their electronic communications.[22]

For Fourth Amendment reasonableness purposes, the question is not merely whether individuals have a privacy interest in the materials searched or seized; the analysis focuses on the extent of the government's *invasion* of those interests.

To understand the degree of privacy invasion caused by Section 702, it is first useful to look at the many significant statutory limitations. The statute explicitly prohibits the government from using Section 702 to intentionally target: (1) "any person known at the time of acquisition to be located in the United States"[23] or (2) "a United States person reasonably believed to be located outside the United States."[24] Section 702 bars the government from intentionally targeting an individual who is located outside of the United States with the ultimate goal of collecting information from a person who is reasonably believed to be located in the United States (a practice known as "reverse targeting").[25] Section 702 also prohibits the government from intentionally acquiring "any communication as to which the sender and all intended recipients

---

[21] Paul Rosenzweig, et al., HERITAGE FOUNDATION, MAINTAINING AMERICA'S ABILITY TO COLLECT FOREIGN INTELLIGENCE: THE SECTION 702 PROGRAM (May 13, 2016).

[22] *See* United States v. Warshak, 631 F.3d 266, 286 (6th Cir. 2010) ("It follows that email requires strong protection under the Fourth Amendment; otherwise, the Fourth Amendment would prove an ineffective guardian of private communication, an essential purpose it has long been recognized to serve."); United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) ("[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers.") (internal citations omitted).

[23] 50 U.S.C. § 1881a(b)(1).

[24] 50 U.S.C. § 1881a(b)(3).

[25] 50 U.S.C. § 1881a(b)(2).

are known at the time of the acquisition to be located in the United States."[26] Moreover, the Government must acquire data under Section 702 in a manner that is "consistent" with the Fourth Amendment.[27]

Further, Section 702 explicitly requires reasonable procedures "to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information."[28] Each agency that has access to Section 702 data has developed detailed minimization procedures.[29]

Section 702 programs are subject to a number of additional procedural safeguards:

First, and most importantly, all three branches of government oversee Section 702. Within the executive branch, the NSA imposes multiple levels of controls on the analysts who target and task communications.[30] Additionally, the Justice Department and Office of the Director of National Intelligence regularly review documentation of NSA analysts' Section 702 activities to ensure compliance.[31] Congress has an active oversight role, with the House and Senate Judiciary and Intelligence Committees receiving regular compliance reviews, certifications, and information related to other key operational aspects of Section 702.[32] Finally, the Foreign Intelligence Surveillance Court, comprised of Article III, life-tenured judges, provides extensive oversight of the program. For instance, in response to a 2011 FISC opinion questioning the sufficiency of certain minimization procedures, NSA revised those procedures.[33] The involvement of all three branches of government in the oversight of this program weighs heavily in any Fourth Amendment analysis.[34]

---

[26] 50 U.S.C. § 1881a(b)(4).
[27] 50 U.S.C. § 1881a(b)(5).
[28] 50 U.S.C. § 1801(h)(1).
[29] For redacted, declassified versions of the minimization procedures implemented by the NSA, FBI, CIA, and NCTC in 2015, see Office of the Director of National Intelligence, IC on the Record, RELEASE OF 2015 SECTION 702 MINIMIZATION PROCEDURES (Aug. 11, 2016), *available at* https://icontherecord.tumblr.com/post/148797010498/release-of-2015-section-702-minimization.
[30] *See* Hoover Paper at 16-17. The NSA and FBI each have targeting procedures, but PCLOB concluded that the NSA's targeting procedures "take primary importance because only the NSA may initiate Section 702 collection" and the FBI's targeting procedures "are applied to certain selectors only after the NSA has previously determined under the NSA targeting procedures that those selectors qualify for Section 702 targeting." PCLOB Report at 42. FBI and CIA may "nominate" targets to the NSA. *Id.*
[31] *See* Hoover Paper at 17-18.
[32] *See* PCLOB Report at 76-77; 50 U.S.C. § 1881f.
[33] Hoover Paper at 19.
[34] *See* PCLOB Report at 92 ("Where, as here, 'the powers of all three branches of government – in short, the whole of federal authority' – are involved in establishing and monitoring the parameters of an intelligence-gathering activity, the Fourth Amendment calls for a different

Second, the Attorney General and Director of National Intelligence must annually certify the purposes of Section 702 operations, and they must attest that "a significant purpose of the acquisition is to obtain foreign intelligence information."[35]

Third, before NSA collects any data through Section 702 from service providers or other companies, it must go through a detailed, multi-step targeting procedure, approved by the Foreign Intelligence Surveillance Court, to ensure that the target of the surveillance is a non-U.S. person.[36] As documented in the PCLOB report, the Justice Department "determined that 0.4% of NSA's targeting decisions resulted in the tasking of a selector that, as of the date of tasking, had a user in the United States or who was a U.S. person."[37] Only after the NSA has targeted, selected, and tasked the communications to service providers will government agencies even have the ability to query any of the data.

Fourth, the government is subject to strict retention and destruction procedures. For example, under the NSA's minimization procedures, if a communication is determined to be a domestic communication, that communication and the entire Internet transaction on which it is contained "will be promptly destroyed upon recognition" unless the NSA Director or Acting Director issues a specific written determination for each communication that the "sender or intended recipient of the domestic communication had been properly targeted under Section 702" *and* at least one of the following conditions is met: (1) the communication is "reasonably believed to contain significant foreign intelligence information;" (2) the communication is "reasonably believed to contain evidence of a crime that has been, is being, or is about to be committed;" (3) the communication is "reasonably believed" to contain technical data base information or information "necessary to understand or assess a communications security vulnerability;" or (4) the communication contains information of an "imminent threat of serious harm to life or property."[38]

Despite these safeguards, critics raise a number of legitimate points regarding potential privacy intrusions under Section 702. I will address what I believe raises the closest Fourth Amendment issue: the FBI's subsequent querying of data that has been validly collected under Section 702's targeting and minimization procedures. After reviewing extensive documentation related to Section 702, the prospect of post-collection queries for evidence of crimes causes me the greatest Fourth Amendment concerns.

The FBI's 2015 minimization procedures permit authorized FBI users to "query FBI electronic and data storage systems that contain raw FISA-acquired information to find, extract, review, translate, and assess whether such information reasonably appears to be foreign intelligence

---

calculus than when the executive branch acts alone.") (quoting United States v. Abu-Jihaad, 630 F.3d 102, 121 (2d. Cir. 2010)).

[35] 50 U.S.C. § 1881a(g)(2)(v).

[36] *See* Hoover Paper at 10-11; PCLOB Report at 44.

[37] PCLOB Report at 44-45 ("The purpose of the review was to identify how often the NSA's foreignness determinations proved to be incorrect. Therefore, the DOJ's percentage does not include instances where the NSA correctly determined that a target was located outside the United States, but post-tasking, the target subsequently traveled to the United States.").

[38] NSA 2015 Minimization Procedures at 12-13.

information, to be necessary to understand foreign intelligence information or assess its importance, or to be *evidence of a crime*."[39] The procedures require that "[t]o the extent reasonably feasible, authorized users with access to raw FISA-acquired information must design such queries to find and extract foreign intelligence information or evidence of a crime" and maintain records of all such queries.[40]

In a Nov. 6, 2015 opinion (released in redacted form to the public in April 2016),[41] Judge Thomas F. Hogan of the Foreign Intelligence Surveillance Court ruled that this process is constitutional during his review of Section 702 certifications and procedures. Judge Hogan only reached that conclusion after hearing thoughtful arguments from court-appointed Amicus Curiae. Amicus argued that under these procedures, "the FBI may query the data using U.S. person identifiers for purposes of any criminal investigation or even an assessment" and that "[t]here is no requirement that the matter be a serious one, nor that it have any relation to national security."[42] Amicus raises a strong criticism of the program: should the FBI be permitted to query the records of a *foreign intelligence* surveillance program for evidence of a crime that might be unrelated to national security?

For Fourth Amendment purposes, the answer to that question largely hinges on precisely which action is being subjected to the reasonableness test. Amicus argued that each FBI query of Section 702 information is a "separate action subject to the Fourth Amendment reasonableness test."[43] Judge Hogan correctly rejected that formulation,[44] and instead adopted the government's proposed test that "the program as a whole" must be evaluated for Fourth Amendment reasonableness.[45] Under this framework, the court must "weigh the degree to which the government's implementation of the applicable targeting and minimization procedures, viewed as a whole, serves its important national security interests against the degree of intrusion on Fourth Amendment-protected interests that results from that implementation."[46]

---

[39] FBI 2015 Minimization Procedures at 11 (emphasis added).
[40] *Id.*
[41] [Redacted Case Title], Memorandum Opinion and Order, Foreign Intelligence Surveillance Court (Nov. 6, 2015), *available at* https://www.dni.gov/files/documents/20151106-702Mem_Opinion_Order_for_Public_Release.pdf (hereinafter, "Hogan Opinion").
[42] *Id.* at 39.
[43] *Id.* at 40.
[44] *See* David S. Kris, *Trends and Predictions in Foreign Intelligence Surveillance: The FAA and Beyond,* 8 J. NAT'L SECURITY L. & POL'Y __ (forthcoming 2016) ("Underlying this debate is an interesting, although somewhat technical, question of whether querying should be seen as a separate, stand-alone Fourth Amendment event, such that it must satisfy constitutional requirements on its own, or whether it is instead best seen as part of the overall Fourth Amendment even described by the FAA, which includes but is not limited to acquisition, retention, querying, and dissemination of information. The former seems to have some support in the historical position of the government going back to the 1980s, but the latter is at least arguably more consistent with more recent authority, particularly in the context of FAA § 702.").
[45] Hogan Opinion at 40-41.
[46] *Id.* at 41.

Applying this analytical framework, Judge Hogan set forth a compelling case as to why national security interests outweigh the intrusion on individual privacy interests. Importantly – and often overlooked in Section 702 debates – is the fact that the FBI and other agencies only can query data that has been obtained through NSA's targeting program. And NSA only can obtain that data if it takes steps "to determine that the user of the selector is a non-United States person who is reasonably believed to be located outside the United States and that he or she is expected to possess, receive, or communicate foreign intelligence information."[47]

Judge Hogan's decision critically relied on the fact that "only a subset" of the Section 702 information is available to the FBI for queries.[48] Importantly, the FBI does not receive unminimized information obtained through NSA's upstream collection process, which is more likely than PRISM to contain non-target communications of U.S. persons or persons located in the United States because upstream collection can include selectors that are found in the body of a communication.[49] Moreover, Judge Hogan wrote that the government has stated that "FBI queries designed to elicit evidence of crimes unrelated to foreign intelligence rarely, if ever, produce responsive results from the Section 702-acquired data."[50]

Therefore, Judge Hogan concluded that "the risk that the results of such a query will be viewed or otherwise used in connection with an investigation that is unrelated to national security appears to be remote, if not entirely theoretical."[51] However, he recognized the need for the Court "to reassure itself that this risk assessment is valid," and therefore began requiring the government to report "any instance in which FBI personnel receive and review Section 702-acquired information that the FBI identifies as concerning a United States person in response to a query that is not designed to find and extract foreign intelligence information."[52] This strikes me as an appropriate safeguard to protect against abuse of the program, and it demonstrates the efficacy of FISC oversight of Section 702.

Similarly, in 2015, a federal judge in Colorado declined to suppress Section 702 evidence in a criminal case against Jamshid Muhtorov, who was charged with providing material support to a designated terrorist organization and conspiracy to do the same.[53] Although Muhtorov challenged a variety of aspects of Section 702, much of his challenge related not to the initial, incidental collection of his communications, but to the subsequent "retention and *use* of those communications by federal law enforcement in criminal proceedings against him in a court of law."[54] Judge John L. Kane explained why this subsequent use is not a discrete "search" under the Fourth Amendment:

---

[47] *Id.*
[48] *Id.* at 43.
[49] PCLOB Report at 35-41; Hogan Opinion at 43-44 (observing that upstream collection is "more likely than others to include non-target communications of United States persons and persons located in the United States that have no foreign intelligence value.")
[50] Hogan Opinion at 44.
[51] *Id.*
[52] *Id.*
[53] United States v. Muhtorov, Criminal Case No. 12-cr-00033-JLK (D. Colo. Nov. 19, 2015).
[54] *Id.* at 29 (emphasis in original).

> Accessing stored records in a database legitimately acquired is not a search in the context of the Fourth Amendment because there is no reasonable expectation of privacy in that information. Evidence obtained legally by one police agency may be shared with similar agencies without the need for obtaining a warrant, even if it sought to be used for an entirely different purpose.[55]

On balance, the FBI's ability to query Section 702 data, as described in the public record, does not render Section 702 unconstitutional. During the reauthorization process, Congress may well conclude that there are legitimate policy reasons to limit the FBI's ability to conduct such queries. However, my testimony today is limited to the application of the Fourth Amendment to Section 702.

Concluding Thoughts

On balance, the important role that Section 702 plays in promoting national security outweighs the intrusions on individual privacy interests. As I stressed at the beginning of my testimony, I did not arrive at this conclusion easily. Indeed, there are many close cases in which strong constitutional arguments can be made for and against elements of the program, most notably when domestic law enforcement subsequently queries Section 702 data for evidence of ordinary crimes. As a matter of Fourth Amendment law, however, we must examine the totality of the program. Section 702 contains vital safeguards, including oversight by this Committee and others as well as the Foreign Intelligence Surveillance Court. Indeed, after its extensive examination of Section 702, PCLOB concluded that "[o]peration of the Section 702 program has been subject to judicial oversight and extensive internal supervision, and the Board has found no evidence of intentional abuse."[56]

I recognize that the Committee is conducting a hearing on Section 702 in the year when it is set to expire, and you likely have many policy options to consider. I am limiting my comments today to whether Section 702 is constitutional, and the other panelists may be better positioned to comment on policy preferences.

I will conclude with one broad observation about the importance of transparency. The intelligence community continues to increase the amount of information available to the public about Section 702, including statistics about the use of Section 702, redacted Foreign Intelligence Surveillance Court Opinions, and minimization procedures.[57] I commend these transparency efforts, which are especially important in supporting an informed public legal and policy debate in the context of foreign intelligence programs that are inherently secretive and classified. Further, the work of PCLOB has been absolutely essential in informing the public debate on Section 702. Indeed, without PCLOB's thorough and transparent evaluation of Section 702, it would be difficult, if not impossible, to evaluate the constitutionality of Section 702. I hope that these transparency efforts continue, because they allow all of us to better do our job at evaluating these vital constitutional issues. The Fourth Amendment – like other important

---

[55] *Id.* at 31.
[56] PCLOB Report at 2.
[57] *See* OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, IC ON THE RECORD, *available at* https://icontherecord.tumblr.com/.

constitutional rights – is highly fact-dependent and requires close analysis of not only how the program is structured by statute, but how it actually is implemented. The public release of information by the intelligence community and public hearings such as this are absolutely vital as we continue to evaluate Section 702 and other intelligence programs.

Mr. GOODLATTE. Thank you.
Ms. Doss, welcome.

TESTIMONY OF APRIL F. DOSS, PARTNER, SAUL EWING LLP

Ms. DOSS. Mr. Chairman, Mr. Ranking Member, Members of the Committee, thank you for the opportunity to testify about Section 702 of the FISA Amendments Act. My name is April Doss. I am a partner at the law firm Saul Ewing. Prior to that, I spent 13 years at the National Security Agency.

Although my perspective is informed by the years I spent in the intelligence community, the views expressed here are solely my own and do not represent the NSA or any other agency or organization.

Like many other Americans, I recall exactly where I was on September 11, 2001, and not long after that I began working at the NSA where over the years I managed counterterrorism programs, conducted intelligence oversight activities, and spent a number of years in the Office of General Counsel, where, among other things, I served as the associate general counsel for intelligence law, responsible for providing legal advice on all of NSA's overseas intelligence operations, technology development used for those operations, and privacy, civil liberties, and oversight and compliance programs.

Having worked at NSA both before and after the passage of the FISA Amendments Act, and having worked with that authority from a number of perspectives, I can attest to the following observations from my personal experience.

In 2008, when the law was passed, the authority was critically needed because of the gaps created by the ways in which technology and intelligence targets had changed in the years since the original FISA was passed, the very points that Mr. Chairman referred to in his opening statement.

The 702 authority strikes an appropriate balance between the government's need for foreign intelligence information and the privacy impacts on individuals, the very same critical points that Mr. Ranking Member pointed to in his opening statement.

The statutory framework incorporates robust oversight requirements and privacy protections. Those protections have been implemented across all three branches of government in meaningful and substantive ways. And the 702 authority has consistently, since its passage in 2008, provided critical intelligence information to the U.S. and to its allies, including intelligence critical to supporting warfighters in the field that would not have been obtainable in other ways.

FISA appropriately balances individual privacy and national security. One point to start with, despite some public misconceptions to the contrary, FAA 702 is a targeted intelligence authority. It's not bulk collection. The collection can only be initiated when an analyst is able to articulate and document a specific set of facts to meet the statutory and procedural requirements for demonstrating that a specific facility is associated with a specific user, who's a non-U.S. person, reasonably believed to be located outside the U.S., and likely to possess or communicate foreign intelligence information.

Although a large number of selectors have been targeted under 702, they've only been tasked for collection because on an individualized, particularized basis each of them meets all of those criteria noted in the law.

And because of the tailored and documented and carefully overseen manner in which the front-end collection is carried out, it's neither unlawful nor inappropriate, in my view, to query that collection for U.S. person information when there's a legitimate basis to do so, and those legitimate bases may include both intelligence purposes and law enforcement purposes, as articulated by Judge Hogan in his November 2015 court opinion.

The government has a compelling national security need to be able to carry out U.S. person searches of that collected information in appropriate cases. As an intelligence community lawyer for many years, I know firsthand just how often urgent, time-sensitive operational needs arise. And I can tell you, it's my view that if it were necessary for intelligence analysts, who work 24 hours a day, 7 days a week, to receive prior approval from somewhere outside of the NSA or the CIA or the FBI, for instance, from the FISC to conduct a query, that could have a significant detrimental impact on intelligence activities.

With respect to the question of estimating the amount of U.S. person information that's incidentally acquired in 702 collection, this is a critically important question that goes to the heart of this balancing between national security and privacy. However, I do believe that it raises significant privacy implications in how that might be done.

The challenge, of course, being how to have the reference information that an intelligence analyst would need to know who the user is of an unknown identifier or where that user is in the world. In my view, the collection and maintenance of that reference information would itself pose significant impacts to privacy.

During 13 years at the NSA, I had the opportunity to witness firsthand the critical importance of this authority in supporting U.S. troops, in detecting terrorist plans and intentions and other critical intelligence needs, and in protecting the U.S. and its allies. Many of those instances remain classified, but the PCLOB's report, I think, points to the importance of that collection and its sheer volume.

Thank you, and I look forward to the Committee's questions.

[The testimony of Ms. Doss follows:]

STATEMENT OF

APRIL F. DOSS

PARTNER, SAUL EWING, LLP

BEFORE THE UNITED STATES HOUSE OF REPRESENTATIVES
JUDICIARY COMMITTEE

CONCERNING

SECTION 702 OF THE
FOREIGN INTELLIGENCE SURVEILLANCE ACT

MARCH 1, 2017

TESTIMONY OF APRIL F. DOSS
PARTNER, SAUL EWING, LLP
BEFORE THE UNITED STATES HOUSE OF REPRESENTATIVES
JUDICIARY COMMITTEE
MARCH 1, 2017

Mr. Chairman, Mr. Ranking Member, and Members of the Committee, thank you for the opportunity to testify about Section 702 of the FISA Amendments Act.

My name is April Doss, and I am a partner in the law firm Saul Ewing, LLP, where I chair the firm's Cybersecurity and Privacy practice group. Prior to that, I spent thirteen years at the National Security Agency, and before that, I worked as a public defender, in private practice, and as in-house counsel. The views that I express today are entirely my own and do not represent those of my firm, the National Security Agency, or any other agency or organization. My views are, however, informed by my experience working in the Intelligence Community, and so I will say a few brief words about those qualifications.

Like many other Americans, I recall exactly where I was on September 11, 2001. As I watched the twin towers collapse, I – like so many others – knew that our world had been irrevocably changed. Not long after that, I applied for a position at the National Security Agency (NSA), where I began working in September 2003.

During thirteen years at NSA, I worked in a variety of capacities. I was a senior policy officer for information sharing during the work of the 9/11 Commission and the passage of the Intelligence Reform and Terrorism Prevention Act. I managed counterterrorism programs and served as a foreign liaison officer. I was an intelligence oversight officer and an intelligence oversight program manager for multi-site intelligence operations. I served on the senior management team for new technology development. I also spent six years in the General Counsel's office at NSA. From 2005-2009, I was what we called an "operations" attorney. I provided legal advice to NSA's intelligence collectors, analysts, reporters, and oversight and compliance officers about the requirements of the Foreign Intelligence Surveillance Act (FISA) and other laws and associated procedures, regulations, and policies; I worked closely with counterparts from the Department of Justice; and I served as principal legal advisor on NSA's efforts to develop the new technology capabilities that would be used to carry out those intelligence activities. During that first stint in NSA's Office of General Counsel (OGC), I observed firsthand the ways in which a changing global telecommunications infrastructure had changed the practical impact of the Foreign Intelligence Surveillance Act. I advised NSA personnel on FISA in its traditional form, as well as on the new authorities and restrictions that came with the passage of the Protect America Act (PAA) in 2007 and the FISA Amendments Act (FAA) in 2008. In 2014, I returned to NSA's legal office, where I served as the Associate General Counsel for Intelligence Law. In that capacity, I led the group of several dozen attorneys responsible for giving legal advice on all of NSA's intelligence activities, including NSA's applications to the Foreign Intelligence Surveillance Court (FISC); NSA's use of the

FAA 702 authority; the technical capabilities being used for NSA's intelligence operations; and NSA's civil liberties, privacy, and oversight and compliance programs, including NSA's reporting to internal and external overseers of incidents of non-compliance. Throughout that time, I worked closely with counterparts at other executive branch agencies, including the Department of Justice (DoJ), the Office of the Director of National Intelligence (ODNI), the Central Intelligence Agency (CIA), and the Federal Bureau of Investigation (FBI). I left government service in April, 2016 in order to take my current position.

Because much of the work that I did during those years was classified at the time, and because of my lifetime security obligations as a previous holder of classified information, this testimony has been submitted to the NSA for prepublication review to ensure that there has been no inadvertent inclusion of information that ought to be properly classified. That review, however, does not impact any of the views expressed in this statement, and all views are solely my own.

Having worked at NSA both before and after the passage of the FISA Amendments Act, and having been involved with that authority from a number of perspectives over the years – as a CT program manager, intelligence oversight program manager, technology policy architect, and legal advisor – I can attest to the following observations from my personal experience:

1) In 2008 when the law was passed, the authority was critically needed by the Intelligence Community because of the gaps created by the ways in which technology had changed in the years since the original FISA was passed;

2) The FAA 702 authority strikes an appropriate balance between the government's need for foreign intelligence information and the privacy impacts on individuals, including the impacts resulting from incidental interception of U.S. person communications;

3) The statutory framework incorporates robust oversight requirements and privacy protections;

4) Those protections have been implemented across all three branches of government in meaningful and substantive ways; and

5) The 702 authority has consistently, since its passage in 2008, provided critical intelligence information to the U.S. and its allies that would not have been obtainable in other ways.

1. THE NEED FOR THE FAA 702 AUTHORITY – THEN AND NOW

As this Committee considers whether to support reauthorization of FAA 702, it is worth revisiting the reasons why Congress chose to enact this legislation in 2008, and to renew it in 2012.

As the Committee is aware, prior to the passage of the short-term PAA legislation in 2007 and the FAA in 2008, the Intelligence Community was required to make individualized

showings of probable cause for each application filed under Title I of the FISA. Under the Title I rubric, the government must articulate a specific case demonstrating that there is probable cause to believe each target is a foreign power or an agent of a foreign power, and that each facility – such as an email address or telephone number – is associated with that foreign power or agent of a foreign power.[1] Title I remains the backbone of the overall FISA framework, but it is a poor fit for certain kinds of intelligence challenges, and its utility had been impacted dramatically by changes in the telecommunications environment between 1978, when FISA was passed, and the early 2000s.

In a post-9/11 world, the nature of intelligence targets, the diffuse nature of threats to the U.S., and the challenges of intelligence gathering all made clear that the Title I FISA approach was a poor fit for tackling some of the hardest intelligence problems, such as counterterrorism and countering the proliferation of weapons of mass destruction, that did not directly involve nation-state adversaries. The 21st century had ushered in a new era of communications in which intelligence targets were no longer primarily found talking on landline phones from within government buildings belonging to adversarial nations, nor were they limited to the radio communications of foreign military units that were being used to communicate troop positions or weaponry movements. Instead, diffuse groups such as terrorist networks now using the same commercial telephone and free webmail services that ordinary people around the world were using to stay in touch with family and friends. Terrorists couldn't be counted on to communicate via landline from fixed geographical positions. They didn't have air forces or naval fleets or conventional military bases full of tanks and troop carriers whose movements could be monitored by more traditional means. Instead, they frequently operated from within ordinary communities; they communicated via ordinary commercial means; they took great pains to hide their identities and their communications. In this new era, terrorists' planning for external operations – that is, their planning for attacks outside of the geographic region where they were based – was frequently concealed by a combination of means which made detection and analysis of those communications extraordinarily difficult to carry out through conventional intelligence collection means.[2]

The FISA requirement for individualized warrants meant that the government's capacity to seek intelligence information was necessarily constrained by the resources that would be required to submit an individualized probable cause application for every target of electronic surveillance. Further, the Title I requirement that collection be limited to foreign powers and agents of foreign powers meant that some valuable intelligence information was inaccessible altogether, either because the government did not yet have sufficient information to support a probable cause determination, or because the individual whose communications were being sought was someone who was likely to possess, receive or communicate foreign intelligence information but who did not meet the statutory definition of a foreign power or agent of a foreign

---

[1] *See generally* 50 U.S.C. §1801-1813.

[2] *See generally*, Hearing before the Senate Select Committee on Intelligence, Sept. 20, 2007, available online at https://www.gpo.gov/fdsys/pkg/CHRG-110jhrg38878/html/CHRG-110jhrg38878.htm ; *see also* Testimony of Kenneth L. Wainstein before the United States Senate Committee on the Judiciary, May 10, 2016, p. 3-5, available online at: https://www.judiciary.senate.gov/imo/media/doc/05-10-16%20Wainstein%20Testimony.pdf .

power.[3] Perhaps worst of all, the changes in telecommunications infrastructure between 1978 and the mid-2000s meant that FISA's language – and Congress's intent – had been turned on its head: where Congress's 1978 language required FISC authorization to collect calls from a wire (calls that would most likely have been landline, local calls in the U.S.) but exempted certain radio communications (international calls), the shift to undersea cables for international communications and the installation of cellular infrastructure meant that by 2007, local calls were carried via radio signal and international calls were conveyed on a wire. Because the statutory language had remained the same, there were now circumstances in which FISA applied in ways that were nearly the opposite of its original intent.[4]

In other words, the protections under Title I of the FISA, which had been designed to protect the Fourth Amendment rights associated with U.S. persons' communications, were having an unintended result by the mid-2000s: they were imposing strict statutory restrictions on the collection of information from and about persons who were not entitled to Fourth Amendment rights, and they were simultaneously preventing the government from obtaining important intelligence information that was constitutionally permissible.

These challenges were described in detail in Congressional hearings on the passage of the FAA in 2008, its reauthorization in 2012, and in hearings held by this Committee[5] and by the Senate Judiciary Committee[6] during the last Congress in advance of the current reauthorization discussion.

The result has been the addition to FISA of the current FAA Section 702 framework in which the government is granted the authority to compel communications providers to assist the government in the acquisition of communications that are to, from, or about persons who are expected to possess, communicate, or receive foreign intelligence information. Those processes are carried out through a comprehensive framework in which the Attorney General and Director of National Intelligence certify areas of foreign intelligence to be gathered; the FISC reviews and approves those certifications; the executive branch serves directives on communications

---

[3] *See* Testimony of Matthew G. Olsen before the Senate Committee on the Judiciary, May 10, 2016, p. 7, available online at: https://www.judiciary.senate.gov/imo/media/doc/05-10-16%20Olsen%20Testimony.pdf

[4] "Because of these changes in technology, communications intended to be excluded from FISA in 1978 were, in fact, frequently included in 2007. This had real consequences. It meant the community in a significant number of cases was required to demonstrate probable cause to a court to collect communications of a foreign intelligence target located overseas." Testimony of Director McConnell before the Senate Select Committee on Intelligence, Sept. 20, 2007, available online at https://www.gpo.gov/fdsys/pkg/CHRG-110jhrg38878/html/CHRG-110jhrg38878.htm .

[5] *See* the Joint Unclassified Statement of Robert S. Litt, General Counsel Office of the Director of National Intelligence; Stuart J. Evans Deputy Assistant Attorney General for Intelligence, National Security Division, Department of Justice; Michael B. Steinbach, Assistant Director Counterterrorism Division, Federal Bureau of Investigation; and Jon Darby, Chief of Analysis and Production, Signals Intelligence Directorate, National Security Agency Before the House Committee on the Judiciary, United States House of Representatives, February 2, 2016, available online at: https://judiciary.house.gov/wp-content/uploads/2016/02/joint-sfr-for-doj-fbi-odni-and-nsa-updated.pdf .

[6] https://www.judiciary.senate.gov/meetings/oversight-and-reauthorization-of-the-fisa-amendments-act-the-balance-between-national-security-privacy-and-civil-liberties

providers; and the intelligence agencies designate and document the individual selectors that meet the detailed criteria required under the statute, certifications, and targeting procedures.[7] The collection is effectuated by two means: 1) through PRISM collection in which electronic communications service providers assist the government in acquiring communications that are to or from targeted selectors, and 2) through "upstream" collection in which telecommunications backbone providers assist the government in acquiring telephony communications to or from a targeted selector and internet transactions that are to, from, or about a targeted selector.[8] The information, once acquired, is handled in accordance with Court-approved minimization procedures that govern the processing, analysis, retention, and dissemination of the data. These minimization procedures are an essential part of the overall set of measures that makes the FAA 702 an appropriately circumscribed program.

2. FAA 702 Appropriately Balances Individual Privacy and National Security

The first and most important point to make is that, despite some public misconceptions to the contrary, FAA 702 is a targeted intelligence authority. It is not "bulk" collection. As explained by the independent Privacy and Civil Liberties Oversight Board (PCLOB) in its July, 2014 report, "The statutory scope of Section 702 can be defined as follows: Section 702 of FISA permits the Attorney General and the Director of National Intelligence to jointly authorize the 1) targeting of persons who are not United States persons, 2) who are reasonably believed to be located outside the United States, 3) with the compelled assistance of an electronic communication service provider, 4) in order to acquire foreign intelligence information."[9]

In more concrete terms, FAA 702 collection can only be initiated when an analyst is able to articulate, and document, a specific set of facts to meet the statutory and procedural requirements for demonstrating that: 1) a specific "facility" (such as a phone number or email address) 2) is associated with a specific user 3) who is a non-U.S. person 4) who is reasonably believed to be located outside the U.S. and 5) who is likely to possess or communicate foreign intelligence information.[10]

Although a large number of selectors have been targeted under FAA 702, each of those selectors has been tasked for collection because *on an individual, particularized basis* each one of them meets the criteria noted above.[11] "Bulk" collection is different: as explained in

[7] *See generally* 50 U.S.C. 1881.

[8] In all cases, PRISM and upstream, the basis for collection is a communications identifier, such as an email address or telephone number. FAA 702 does not authorize, and is not used for, the collection of communications based on key words, names, or generic terms. *See* PCLOB report, p. 33-41.

[9] PCLOB Report, p. 20, citing 50 U.S.C. §1881a(a), 1881a(b)(3), 1881a(g)(2)(A)(vi).

[10] *See* 50 U.S.C. §1881a(a),(b); *see also* Semi-Annual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702, August, 2013, p. A-1- A-2, available online at: https://www.dni.gov/files/documents/Semiannual%20Assessment%20of%20Compliance%20with%20procedures%20and%20guidelines%20issued%20pursuant%20to%20Sect%20702%20of%20FISA.pdf; *and see* Oversight Summary prepared by Department of Justice and Office of the Director of National Intelligence, Aug. 11, 2016, p. 2, available online at: https://icontherecord.tumblr.com/post/148796781888/release-of-a-summary-of-doj-and-odni-oversight-of .

[11] *See* PCLOB Report, p. 103.

"Presidential Policy Directive – Signals Intelligence Activities" (PPD-28), bulk collection is information that is collected without the use of discriminants.[12] This is a critically important difference. As the PCLOB noted in its report, Section 702 does not authorize bulk collection.[13]

Further, once the information has been collected under FAA 702, the information is subject to a significant number of post-collection safeguards that are captured in lengthy, detailed minimization procedures that demonstrate both the care that is taken with the information, and the complexity of the 702 framework.[14] At a high level, the procedural protections include both technical and administrative means. For example, 702 information in stored in restricted-access information systems where the data can be identified as having been collected under, and being subject to, FAA 702 minimization procedures. NSA personnel are only permitted to access the information if they have taken specialized training on those procedures, passed the associated training exam, and have continued to update their training and pass the associated tests on an annual basis. Similar requirements exist for CIA and FBI personnel.[15] Many of these protections are detailed in documents issued by DoJ and ODNI, and I discuss some of these protections in further detail below.

Because of the tailored, documented, and carefully overseen manner in which the front-end collection is carried out, it is neither unlawful nor inappropriate for intelligence analysts to query the collected information using U.S. person identifiers when there is a legitimate basis to do so. Some critics have referred to the ability to query 702 data for U.S. person information as "back door searches." That hyberbolic phrase doesn't help illuminate the true issues – the intelligence benefits or the privacy risks – that are stake. First, it is important to understand how such queries actually happen. As the PCLOB noted in its report, the use of query terms relating to U.S. persons is tightly constrained at both NSA and CIA, which have similar practices; FBI takes a different approach.[16] I'm most familiar with NSA's processes: NSA analysts must obtain prior approval to run U.S. person identifier queries in FAA 702 content; there must be a basis to believe the query is reasonably likely to return foreign intelligence information; all

---

[12] PPD-28 notes that, "References to signals intelligence collected in "bulk" mean the authorized collection of large quantities of signals intelligence data which, due to technical or operational considerations, is acquired without the use of discriminants (e.g., specific identifiers, selection terms, etc.)." https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities#_ftn5

[13] PCLOB Report at 103, available online at: https://www.pclob.gov/library/702-Report.pdf .

[14] These procedures have been declassified, with minor redactions, and released for public review. For example, the 2014 procedures include NSA Section 702 Minimization Procedures, available online at: https://www.dni.gov/files/documents/0928/2014%20NSA%20702%20Minimization%20Procedures.pdf . The FBI Section 702 Minimization Procedures are available online at: https://www.dni.gov/files/documents/0928/2014%20FBI%20702%20Minimization%20Procedures.pdf . The CIA Minimization Procedures are available online at: https://www.dni.gov/files/documents/0928/2014%20CIA%20702%20Minimization%20Procedures.pdf and the NCTC Minimization Procedures are available online at: https://www.dni.gov/files/documents/0928/2014%20NCTC%20702%20Minimization%20Procedures.pdf .

[15] *See* PCLOB Report at p. 53, 127, available online at: https://www.pclob.gov/library/702-Report.pdf.

[16] PCLOB Report at p. 129-131, available online at: https://www.pclob.gov/library/702-Report.pdf.

queries are logged and reviewed after the fact by NSA; and DoJ and ODNI review every U.S. person query run at NSA and CIA, along with the documented justifications for those queries.[17]

As a practical matter, internal agency mechanisms also provide strong protections against abuse. For example, within the NSA intelligence oversight framework, query auditors and intelligence oversight officers play an active role in checking for errors or unauthorized queries. Throughout my time at NSA, I routinely saw analysts self-report if they ran an improper query; auditors actively review and assess query logs for any indication of any improper query; and questionable queries are reported promptly to NSA's internal intelligence oversight officers and organizations for further action, which includes reporting to external overseers.

Writ large, the government has put in place detailed mechanisms to protect individual privacy within the 702 framework, including measures to guard against the overuse or improper use of queries the deliberately search for U.S. person information in Section 702 data.

3. THE STATUTORY FRAMEWORK ESTABLISHES ROBUST AND EFFECTIVE OVERSIGHT MECHANISMS

In designing this statute, Congress wisely chose to build in oversight mechanisms involving all three branches of government.

Four committees of Congress have oversight jurisdiction of the government's activities under Section 702: this Committee, the Senate Committee on the Judiciary, the Senate Select Committee on Intelligence, and the House Permanent Select Committee on Intelligence. The statute requires the Attorney General to provide Congress with a semiannual report assessing the government's compliance with the targeting and minimization procedures of the 702 program, along with additional information regarding compliance with the statutory constraints on targeting.[18] As noted by the PCLOB in its 2014 Report, "In practice, the government provides the four committees all government filings, hearing transcripts, and FISC orders and opinions related to the court's consideration of the Section 702 certifications," along with any reports by agency inspectors general.[19]

The FISC also plays a central and critical role in oversight of the 702 program. Under the requirements of the program's procedures and the rules of the FISC, the government must report compliance incidents either immediately upon recognition or as part of quarterly reporting.[20]

---

[17] Oversight Summary prepared by Department of Justice and Office of the Director of National Intelligence, Aug. 11, 2016, p. 3, 4, available online at: https://icontherecord.tumblr.com/post/148796781888/release-of-a-summary-of-doj-and-odni-oversight-of

[18] 50 U.S.C. § 1881b, 1881f, 1881l.

[19] PCLOB Report at 77.

[20] *See* FISC Rules of Procedure, available online at: http://www.fisc.uscourts.gov/rules-procedure Specifically, Rule 13(b), "Disclosure of Non-Compliance" states that, "If the government discovers that any authority or approval granted by the Court has been implemented in a manner that did not comply with the Court's authorization or approval or applicable law, the government, in writing, must immediately inform the Judge to whom the submission was made of: 1) the non-compliance; 2) the facts and circumstances relevant to the non-compliance; 3) any modifications the government has made or proposes to make in how it will implement any authority or approval

These "13(b)" notices contain comprehensive details about the nature of each incident of non-compliance, and are filed promptly and routinely. It is not uncommon for the FISC to ask the government to provide supplemental information, in writing or through in-person briefings, to address any questions that the court may have regarding those incidents. In addition to carrying out this ongoing oversight function, each year, the FISC reviews the government's annual certification package for sufficiency, making independent determinations about whether the proposed certifications meet the necessary standards set forth under the law; whether the targeting and minimization procedures faithfully incorporate all of the restrictions necessary to ensure that they are consistent with the statute and with constitutional requirements; and reviewing the compliance incidents that have taken place over the past year. Each of those compliance incidents will have been previously reported to the FISC, either upon recognition or as part of quarterly reporting. However, the annual certification package provides the FISC with an opportunity to review in total the compliance incidents over the course of a year, to assess whether any trends can be identified or whether there are particular issues that are cause for concern, and to hold the government to account for providing additional information on the nature of those incidents, any steps that might have prevented them from happening, and the details of any remedies that the government may have put in place to correct them or prevent similar occurrences in the future. Further evidence of the FISC's close attention to and careful scrutiny of the government's activities under FAA Section 702 can be found in the court's November 6, 2015 Memorandum Opinion and Order regarding the 2015 FISA Section 702.[21]

It would also be useful to consider here a potential component of oversight that *isn't* currently required by the statute. Members of this Committee, along with others, have asked the government for information regarding the number of U.S. person communications that are collected through the use of the FAA 702 authority. I'd like to offer here some perspective on the practical, policy, and privacy obstacles to making such a count.

As noted above, when the government collects communications under FAA 702, it stores those communications in databases or systems that protect the collected information from unauthorized access, that support queries of the textual information and support the ability to listen to telephonic communications, and that log queries into the systems so that they can be reviewed for lawfulness and consistency with policy. All of these processes are designed around the goal of producing foreign intelligence information, *not* around an intention to look for U.S. person information. Although in theory such searches for U.S. person information could be made, the process of identifying which unknown identifiers are associated with U.S. persons would require the Intelligence Community to deliberately hold and analyze information about U.S. persons, information that it would otherwise have no reason to collect or retain.

Imagine, for a moment, the communications of a non-U.S. person outside the U.S. who is believed to be associated with international terrorism. Further imagine that selectors associated with that person were targeted under Section 702. Once that information has been collected and stored in a database, it can be queried by appropriately cleared and trained analysts. The

---

granted to it by the Court; and 4) how the government proposes to dispose of or treat any information obtained as a result of the non-compliance."

[21] https://www.dni.gov/files/documents/20151106-702Mem_Opinion_Order_for_Public_Release.pdf

analyst's query will be designed to search for those communications that have intelligence value. As they review those communications, they will almost certainly encounter other identifiers – other emails addresses, phone numbers, and the like – that the tasked selector is in communication with, but that are unfamiliar to the analyst. The analyst would need additional information in order to assess whether those unknown identifiers are being used by people in the U.S., or by U.S. persons anywhere in the world. In some cases, technical information may help assist with the location determination. But technical information generally cannot identify whether the user of an email account happens to be a U.S. person located somewhere else in the world. If the communication itself appears to have no intelligence value, the analyst has little reason to research the possible identity, nationality or location of that identifier.

The minimization procedures anticipate precisely how to address this situation: when an analyst determines that a communication contains information that should be disseminated in an intelligence report, the analyst will assess whether the other identifiers are relevant to the intelligence (in some cases, they are not). If not, the report will be written in a way that omits mention of that identifier. If the identifier is relevant, the analyst will look for any indications that the non-target communicant is a U.S. person or a person in the U.S. If that's the case, then that identifier or user's identity (if known) may be masked in any resulting reports. This approach complies fully with the 702 minimization procedures.

From a policy and privacy perspective, the current approach – in which analysts only research unknown identifiers when they appear likely to be of intelligence interest – is a sound and sensible one that protects privacy, conserves resources, and helps the government focus on the highest intelligence priorities. A requirement to count the number of U.S. person communications that are incidentally acquired under Section 702 would require the Intelligence Community to conduct exhaustive analysis of every unknown identifier in order to determine whether they are being used inside or outside the U.S., and whether their users might be U.S. persons located anywhere in the world. NSA does not – nor should it – collect or maintain comprehensive directories of the communications identifiers used by U.S. persons. However, in order to perform a reliable count of U.S. person communications in 702 collection, the Intelligence Community would have to create and maintain precisely such a database. The very creation of these reference databases would constitute an unnecessary and unwarranted intrusion on the privacy of U.S. persons; without specific statutory authorization, it would likely also be unlawful, since it would be both intrusive and unrelated to any need for foreign intelligence gathering.[22] Further, searching for U.S. person information would require intelligence agencies to divert scarce analyst time and computing resources away from intelligence activities in order to hunt for the communications of U.S. persons whose information is not related to an authorized intelligence need (and whose information would never be looked at by the government but for this requirement). Finally, it is unlikely that knowing the number or percentage of U.S. persons in a particular sample of data would result in increased privacy protections in the future: first, because target sets vary over time, and therefore it isn't clear whether numbers or percentages of incidental collection would be constant over time; and second, because the fundamental challenge remains an intractable one: as long as foreign intelligence targets communicate with

[22] Even with statutory authorization, the creation of such a comprehensive database would raise Constitutional concerns.

U.S. persons, it will not be possible to avoid the incidental collection of those specific communications.[23] The best way to protect the privacy of incidental U.S. person communications is to advise analysts that they should *not* proactively search for communications that lack intelligence value, nor conduct exhaustive research to determine whether the unknown communicants in irrelevant communications might be U.S. persons or persons in the U.S.

A middle-ground approach to this challenge is the most appropriate one. The currently implemented practice, adopted in response to PCLOB recommendations and consistent with the USA FREEDOM Act, of reporting on the number of U.S. person queries and the number of disseminations of nonpublic information relating to U.S. persons[24] are appropriate measures that should be continued. The recommendation to report on instances of U.S. person information when it is found and identified as such is one that will impose additional resource burdens on the government but could be another measured and balanced approach to this problem, particularly if used for sampling or for a limited period of time.[25] However, requiring a proactive search through 702 databases for all information relating to U.S. persons would – because of the information it would require the government to collect and hold and because of the resources that would be diverted – be unreasonably intrusive on privacy and ill-advised.

4. SECTION 702 OVERSIGHT IS IMPLEMENTED IN COMPREHENSIVE, THOROUGH WAYS

In addition to being structurally sound, the oversight mechanisms for FAA 702 function robustly in practice. The intelligence agencies have rigorous internal oversight and compliance programs. DoJ and ODNI are deeply engaged in detailed scrutiny of targeting decisions, queries, minimization, and compliance incidents. The FISC is actively involved in oversight and is extremely well equipped to do so: the life-tenured federal judges who are appointed to serve on the FISC demonstrate independence from the Executive and Legislative branches of government, as well as independence from each other. In addition, FISC judges are ably supported by court advisors who, on the judges' behalf, press the government for additional information that may be relevant or necessary to understanding a particular court filing or compliance incident report. Further, the USA Freedom Act brought with it the mechanism for naming independent attorneys as amicus curiae, available to be called upon to provide briefings to the FISC in its consideration of novel matters. Finally, of course, there is the legislative branch, where this Committee plays a vital role.

---

[23] Here, it's important to remember that incidental collection doesn't sweep in all of the communications of a particular U.S. person. It only picks up those specific instances in which that U.S. person has been in communication with a foreign intelligence target. All other communications of that U.S. person remain unaffected, and uncollected.

[24] *See* Privacy and Civil Liberties Oversight Board, Recommendations Assessment Report, February 5, 2016, Recommendation 9, "Adopt Measures to Document and Publicly Release Information Showing How Frequently the NSA Acquires and Uses Communications of U.S. Persons and People Located in the United States," available online at: https://www.pclob.gov/library/Recommendations_Assessment_Report_20160205.pdf .

[25] Tracking indefinitely the instances in which incidental collection is identified as being associated with U.S. persons could, over time, raise new privacy concerns associated with the government's creation and retention of databases of information relating to U.S. persons who are not intelligence targets.

It may be useful to offer additional details about the practical oversight that takes place within the executive branch. These oversight mechanisms have been described in detail in a number of reports[26] as well as an August, 2016 memo issued by DoJ and ODNI.[27] The summary below draws on many of these publically available sources, as well as my own experience with oversight mechanisms for FAA 702.

The joint intelligence oversight reviews conducted by DoJ and ODNI include review of a broad and comprehensive range of detailed documentation regarding the day-to-day implementation of intelligence activities under FAA 702. These include NSA and FBI targeting decisions; reviewing U.S. person identifiers approved by NSA for querying unminimized 702 data; reviewing CIA content queries of unminimized FAA 702 data; reviewing FBI queries of unminimized FAA 702 data; reviewing disseminations of 702 data by NSA, FBI, and CIA; reporting to the FISC and to Congress every instance of non-compliance that is identified; and assessing the Intelligence Community's implementation of appropriate remedial actions to address compliance matters, including purging of non-compliant data and recalling non-compliant disseminations.[28]

At bimonthly visits (often referred to as "60-day reviews"), DoJ and ODNI scour through detailed documentation of targeting decisions, queries, and reporting. NSA prepares exhaustively for these visits, pulling together detailed information on targeting rationales, targeting sheets, query records, and intelligence product reporting. DoJ and ODNI meet with NSA's attorneys and oversight and compliance officers, as well as with analysts and technology personnel as needed in order to answer questions. These 60-day reviews are by no means the only interactions on 702; there are near-daily phone calls, emails, and in-person discussions among NSA, DoJ, and ODNI about current and potential operational and compliance matters, whether those are upcoming reviews, follow-up questions, potential incidents that are being investigated, authorization discussions, or other matters. The dialogue is a robust, continuous, and ongoing one in which DoJ and ODNI both maintain independent professional judgment and distance from the people and organizations they are responsible to oversee. Because the tone of interactions can't be easily captured with metrics, it's hard to convey just how thorough and exhaustive the oversight is, beyond providing this Committee with the observation that I have consistently seen the Department of Justice and ODNI approach their oversight responsibilities with rigor, thorough attention to detail, and a dogged and fully formed intent to ferret out any indication of actual or potential error. Although my direct experience, of course, lies with NSA,

[26] Among the most important sources are the PCLOB's "Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act", July 2, 2014, available online at: https://www.pclob.gov/library/702-Report.pdf and the "Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence" and the Office of the Director of National Intelligence's "Assessment of Oversight & Compliance with Targeting Procedures"; these reports are available online at: https://icontherecord.tumblr.com/post/155810963663/release-of-joint-assessments-of-section-702 .

[27] https://icontherecord.tumblr.com/post/148796781888/release-of-a-summary-of-doj-and-odni-oversight-of

[28] Oversight Summary prepared by Department of Justice and Office of the Director of National Intelligence, Aug. 11, 2016, available online at: https://icontherecord.tumblr.com/post/148796781888/release-of-a-summary-of-doj-and-odni-oversight-of .

Mr. GOODLATTE. Thank you, Ms. Doss.

Regrettably, we're going to have to recess for votes that are on the floor with about 5 minutes remaining in the call. And there are several votes, so it may be a little bit of time. So if you haven't had anything to eat or want take a break, please do so.

We will reconvene as soon as the votes conclude. We'll say 45 minutes. We'll come back just as soon as we possibly can and work through this. And while we're over there, we'll encourage our colleagues to come join us.

Thank you. The Committee will stand in recess.

[Recess.]

[3:38 p.m.]

Mr. MARINO [presiding]. The Judiciary Committee will come to order. And I believe that, Ms. Goitein, you're up next.

TESTIMONY OF ELIZABETH GOITEIN, CO-DIRECTOR, LIBERTY & NATIONAL SECURITY PROGRAM, BRENNAN CENTER FOR JUSTICE, NYU SCHOOL OF LAW

Ms. GOITEIN. Mr. Chairman, Members of the Committee, thank you for this opportunity to testify on behalf of the Brennan Center for Justice.

Congress' goal when it passed the FISA Amendments Act in 2008 was to give our government more powerful tools to use against foreign threats. Consistent with that goal, Section 702 of the act has been used to monitor suspected terrorists overseas, to trace their networks, and to disrupt their plots. All of us in this room, I imagine, support that goal and those activities.

We're here today because of the other things that Section 702 has been interpreted to allow. The government is not simply monitoring foreign terrorists and foreign suspects. Instead, it's scanning the content of almost all of the international communications that flow into and out of the United States and is acquiring hundreds of millions of communications each year.

We know from how the data is collected that it includes a massive amount of Americans' communications. But despite repeated requests by Members of this Committee, the government still has not managed to provide an estimate of how many Americans' communications are swept up.

We also know that despite being required to minimize the retention and use of Americans' data, the government keeps that data for years and routinely searches it for information to use against Americans in ordinary criminal proceedings. According to the Privacy and Civil Liberties Oversight Board, the FBI searches the data when performing assessments, which are investigations that lack a factual predicate. That means the FBI is reading Americans' emails and listening to their phone calls without a factual basis to suspect wrongdoing, let alone a warrant.

I don't believe this is what Congress had in mind when it passed Section 702. In writing the law, however, Congress did give significant discretion to the executive branch and the FISA court, trusting them to implement the statute in a manner consistent with its objective. So for instance, Congress allowed the targeting of any foreigner overseas, trusting the government to focus its efforts on those who pose a threat to us. Congress also left it to the executive

branch and the FISA court to come up with specific minimization rules.

I don't mean to imply that this trust was misplaced. In fact, we've seen essentially no evidence of intentional misuse. But what we have seen is mission creep, so that a law designed to protect against foreign threats to the United States has become a major source of warrantless access to Americans' data and a tool for ordinary domestic law enforcement. This outcome is contrary not only to the original intent of FISA, but to Americans' expectations and their trust that Congress will protect their privacy and their freedoms.

As it now stands, law-abiding citizens of this country and others are vulnerable. Their personal information sits in massive databases where it's subject to being hacked by the Russian or Chinese Government, cyber criminals, or, I suppose, a 400-pound hacker sitting on his bed.

American technology companies are facing the real threat that they'll be unable to do business with foreign companies and customers because of our government's collection practices.

And yes, there is the potential for abuse. Remember that Congress passed FISA in 1978 because multiple Presidents had abused surveillance authorities to target political opponents, personal enemies, and disfavored ideologies and minority groups. In today's tumultuous political environment, we would be naive to think that could never happen again.

We can't rely on the courts to supply the missing protections. The few judges that have reviewed Section 702 have upheld it. They're not delusional. They're not "so-called judges." But they are applying Fourth Amendment precedent and doctrines that are hopelessly unsuited to the digital globalized era. This is a classic case of the law failing to keep up with technology.

When that's happened in the past, Congress has acted to fill the gap. Just a few weeks ago, as you know, the House, by unanimous voice vote, passed the Email Privacy Act. Americans are counting on you to do the exact same thing here, to protect the privacy of their emails and other communications.

Thank you, and I look forward to taking your questions.

[The testimony of Ms. Goitein follows:]

STATEMENT OF

ELIZABETH GOITEIN
CO-DIRECTOR, LIBERTY AND NATIONAL SECURITY PROGRAM
BRENNAN CENTER FOR JUSTICE AT NEW YORK UNIVERSITY SCHOOL OF LAW

BEFORE THE

UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON THE JUDICIARY

HEARING ON

SECTION 702 OF THE FISA AMENDMENTS ACT

MARCH 1, 2017

Introduction

Chairman Goodlatte, Ranking Member Conyers, and members of the committee, thank you for this opportunity to testify on behalf of the Brennan Center for Justice at New York University School of Law.[1] The Brennan Center is a nonpartisan law and policy institute that seeks to improve our systems of democracy and justice. I co-direct the Center's Liberty and National Security Program, which works to advance effective counterterrorism policies that respect constitutional values and the rule of law.

Congress's goal, when it passed the FISA Amendments Act in 2008 (thus creating Section 702 of FISA), was to give our government more powerful tools to address terrorist threats. In keeping with this goal, the authorities conferred by Section 702 have been used to monitor suspected terrorists overseas in order to trace their networks and interrupt their plots. This use of the law is widely recognized as appropriate and has caused little controversy.

In writing the law, however, Congress did not expressly limit Section 702 surveillance to such activities. Instead, Congress gave significant discretion to the executive branch and the FISA Court, trusting them to ensure that the law was implemented in a manner consistent with its objective. For instance, Congress allowed the government to target *any* foreigner overseas, counting on intelligence agencies to focus their efforts on those who pose a threat to our interests. Congress also did not specify what minimization should look like, leaving that to the agencies and the judges of the Foreign Intelligence Surveillance Court.

It would be wrong to suggest that this trust has somehow been betrayed. There has been very little evidence of intentional abuse or misuse. The executive branch, however, has taken full advantage of the leeway provided in the statute. Instead of simply acquiring the communications of suspected terrorists or foreign powers overseas, the government is scanning the content of nearly all of the international communications that flow into and out of the United States via the Internet backbone, and is acquiring hundreds of millions of these communications each year. Based on the manner in which the data is collected, this surveillance inevitably pulls in massive amounts of Americans' calls and e-mails.

We have also seen mission creep. A statute designed to protect against foreign threats to national interests has become a major source of warrantless access to Americans' data, and a tool for ordinary domestic law enforcement. This outcome is contrary, not only to the original intent of the Foreign Intelligence Surveillance Act, but to Americans' expectations and their trust that Congress will protect their privacy and freedoms. It is now up to Congress to enact reforms that will provide such protection.

---

[1] This testimony is submitted on behalf of a Center affiliated with New York University School of Law but does not purport to represent the school's institutional views on this topic. More information about the Brennan Center's work can be found at http://www.brennancenter.org.

I. Background: How Changes in Technology and the Law Led to a Massive Expansion in Government Surveillance

Technological advances have revolutionized communications. People are communicating at a scale unimaginable just a few years ago. International phone calls, once difficult and expensive, are now as simple as flipping a light switch, and the Internet provides countless additional means of international communication. Globalization makes such exchanges as necessary as they are easy. As a result of these changes, the amount of information about Americans that the NSA intercepts, even when targeting foreigners overseas, has exploded.[2]

But instead of increasing safeguards for Americans' privacy as technology advances, the law has evolved in the opposite direction since 9/11. In its zeal to bolster the government's powers to conduct surveillance of foreign threats, Congress has amended surveillance laws in ways that increasingly leave Americans' information outside their protective shield (the USA FREEDOM Act being the notable exception). Section 702 is a particularly striking example.

Before 2007, if the NSA, operating domestically, sought to collect a foreign target's communications with an American inside the U.S., it had to show probable cause to the Foreign Intelligence Surveillance Court (FISA Court) that the target was a foreign power – such as a foreign government or terrorist group – or its agent. The Protect America Act of 2007 and the FISA Amendments Act of 2008 (which created Section 702 of FISA) eliminated the requirement of an individualized court order. Domestic surveillance of communications between foreign targets and Americans now takes place through massive collection programs that involve no case-by-case judicial review.[3]

In addition, the pool of permissible targets is no longer limited to foreign powers or their agents. Under Section 702, the government may target for foreign intelligence purposes any person or group reasonably believed to be foreign and located overseas.[4] The person or group need not pose any threat to the United States, have any information about such threats, or be suspected of any wrongdoing. This change not only renders innocent private citizens of other nations vulnerable to NSA surveillance; it also greatly increases the number of communications involving Americans that are subject to acquisition – as well as the likelihood that those Americans are ordinary, law-abiding individuals.

Further expanding the available universe of communications, the government and the FISA Court have interpreted Section 702 to allow the collection of any communications to, from, *or about* the target.[5] The inclusion of "about" in this formulation is a dangerous leap that finds no basis in the statutory text and little support in the legislative history. In practice, it has been

---

[2] *See* ELIZABETH GOITEIN & FAIZA PATEL, BRENNAN CTR. FOR JUSTICE, WHAT WENT WRONG WITH THE FISA COURT 19-21 (2015), https://www.brennancenter.org/sites/default/files/analysis/What_Went_%20Wrong_With_The_FISA_Court.pdf.

[3] *See* 50 U.S.C. § 1881a.

[4] 50 U.S.C. § 1881a(b).

[5] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 37 (2014) [hereinafter PCLOB 702 REPORT], *available at* https://s3.amazonaws.com/s3.documentcloud.org/documents/1211947/pclob-section-702-report-pre-release.pdf.

applied to collect communications between non-targets that include the "selectors" associated with the target (e.g., the target's e-mail address or phone number). In theory, it could be applied even more broadly to collect any communications that even mention ISIS or a wide array of foreign leaders and public figures who are common topics of conversation. Although the NSA is prohibited from intentionally acquiring purely domestic communications, such acquisition is an inevitable result of "about" collection.

Other than the foreignness and location criteria (and certain requirements designed to reinforce them), the only limitation on collection imposed by the statute is that the government must certify that acquiring foreign intelligence is a significant purpose of the collection.[6] FISA's definition of foreign intelligence, however, is not limited to information about potential threats to the U.S. or its interests. Instead, it includes information "that relates to . . . the national defense or the security of the United States; or . . . the conduct of the foreign affairs of the United States."[7] This could encompass everyday conversations about current events. A conversation between friends or colleagues about the merits of the North American Free Trade Agreement or whether the United States should build a wall along the border with Mexico, for instance, "relates to the conduct of foreign affairs." Moreover, while a significant purpose of the program must be the acquisition of foreign intelligence, the primary purpose may be something else altogether.[8] Finally, the statute requires the FISA Court to accept the government's certifications under Section 702 as long as they contain the required elements.[9] These factors greatly weaken the force of the "foreign intelligence purpose" limitation.

The government uses Section 702 to engage in two types of surveillance. The first is "upstream collection," whereby the content of communications flowing into and out of the United States on the Internet backbone is scanned for selectors associated with designated foreigners. As noted above, the acquired communications include not only communications to or from the designated foreigners, but communications *about* them. Although the data are first filtered in an attempt to weed out purely domestic communications, the process is imperfect and domestic communications are inevitably acquired.[10] The second type of Section 702 surveillance is "PRISM collection," under which the government provides selectors, such as e-mail addresses, to U.S.-based electronic communications service providers, who must turn over any communications to or from the selector.[11] Using both approaches, the government collected more than 250 million Internet transactions a year as of 2011.[12]

Due to these changes wrought by Section 702, it can no longer be said that FISA is targeted at foreign threats. To describe surveillance that acquires 250 million Internet communications a year as "targeted" is to elevate form over substance. And on its face, the statute does not require that the targets of surveillance pose any threat, or that the purpose of the program be the collection of threat information.

---

[6] 50 U.S.C. § 1881a(g)(2)(A)(v).
[7] 50 U.S.C. § 1801(e)(2).
[8] *In re* Sealed Case, 310 F.3d 717, 734 (FISA Ct. Rev. 2002).
[9] 50 U.S.C. § 1881a(i)(3)(A).
[10] PCLOB 702 REPORT, *supra* note 5, at 36-41.
[11] *Id.* at 33-34.
[12] [Redacted], 2011 WL 10945618, at *9 (FISA Ct. Oct. 3, 2011).

Congress no doubt trusted that the executive branch would exercise these broad powers judiciously, and would not conduct surveillance of innocent private citizens abroad simply because the statute, on its face, allows it. And it is certainly possible that the government has chosen to focus its surveillance more narrowly than Section 702 requires. The certifications that the government provides to the FISA Court – which include the foreign intelligence categories at which surveillance is aimed, and could therefore shed some light on this question – have not been publicly disclosed by the government.

Even assuming that actual practices stop short of what the law allows, however, the available statistics suggest a scope of surveillance that is difficult to reconcile with claims of narrow targeting. A leaked copy of one of the certifications, listing the foreign nations and factions about which foreign intelligence may be sought, lends support to the conclusion that surveillance is in practice quite broad: it includes most of the countries in the world, ranging from U.S. allies to small countries that play little role on the world stage.

More important, Americans' privacy should never depend on any given administration's voluntary self-restraint, or on the hope that the FISA Court will impose additional requirements beyond those laid out in the statute. Section 702 establishes the boundaries of permissible surveillance, and it clearly allows collection of communications between Americans and foreigners who pose no threat to the U.S. or its interests. That creates an enormous opening for unjustified surveillance.

II. Constitutional Concerns

The warrantless acquisition of millions of Americans' communications presents deep Fourth Amendment concerns. The communications obtained under Section 702, like any e-mails or phone calls, include not only mundane conversations, but the most private and personal confidences, as well as confidential business information and other kinds of privileged exchanges. Since the Supreme Court decided *Katz v. United States* in 1967, the government has been required to obtain a warrant to wiretap Americans' communications.[13] Moreover, in a subsequent case, the Court made clear that this requirement applied in domestic national security cases as well as criminal cases.[14]

A. "Incidental" Collection

The government nonetheless justifies the warrantless collection of international communications under Section 702 on the ground that the targets themselves are foreigners overseas, and the Supreme Court has held (in a different context) that the government does not need a warrant to search the property of a non-U.S. person abroad.[15] Although the communications obtained under Section 702 sometimes involve both foreigners and Americans,

[13] 389 U.S. 347 (1967).
[14] United States v. U.S. Dist. Court for the E. Dist. Of Mich. (*Keith*), 407 U.S. 297 (1972).
[15] *See* United States v. Verdugo-Urquidez, 494 U.S. 259 (1990).

the FISA Court, along with federal courts in two circuits,[16] have held that the authority to conduct warrantless surveillance of the foreign target entails the authority to "incidentally" collect the communications of those in contact with the target.

Outside of Section 702, however, the case law does not support the existence of a right to warrantless "incidental" collection. The courts reviewing Section 702 have relied on a line of cases dating back to the 1970s, sometimes called the "incidental overhear" cases, in which defendants challenged Title III wiretap orders on the ground that they did not name everyone whose communications might be recorded. The courts held that a warrant meets the Fourth Amendment's "particularity" requirement as long it specifies the phone line to be tapped and the conversations to be acquired, and if the government takes reasonable steps to avoid recording "innocent" conversations.[17] It is hard to see how these rulings on the criteria for a valid warrant could justify *warrantless* collection of Americans' communications.[18]

If, on the other hand, the courts reviewing Section 702 have correctly interpreted the rule emerging from the "incidental overhear" cases, then applying that rule in the Section 702 context would be a classic case of the law failing to keep up with technology. A blanket rule that no warrant is needed for Americans who are in contact with a lawfully surveilled target might have made sense in the 1970s, when there was almost certainly a warrant for the target himself (given the infrequency of international communication) and when government agents monitored the wiretap in real time so that they could turn off the recording equipment if "innocent conversations" were taking place. That rule does not sufficiently protect Americans' reasonable expectation of privacy in an era where millions of Americans communicate with foreigners overseas on a routine basis, those communications can easily be intercepted in massive amounts without any warrant, and there is no mechanism for "turning off" the collection of "innocent communications." Equating the incidental surveillance that takes place in these materially different contexts is like equating "a ride on horseback" with "a flight to the moon."[19]

B. The Foreign Intelligence Exception

Alternatively, the FISA Court (and, more recently, a district court following its lead[20]) has relied on the "foreign intelligence exception" to the Fourth Amendment's warrant requirement. The Supreme Court has never recognized this exception, and there is significant controversy over its scope. The FISA Court has construed the exception extremely broadly,

---

[16] *See* United States v. Mohamud, 843 F.3d 420 (9th Cir. 2016); United States v. Hasbajrami, No. 11-CR-623 (JG), 2016 WL 1029500 (E.D.N.Y. Mar. 8, 2016); *In re* Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1015 (FISA Ct. Rev. 2008).

[17] *See, e.g.*, United States v. Donovan, 429 U.S. 413 (1977); United States v. Kahn, 415 U.S. 143 (1974); United States v. Figueroa, 757 F.2d 466 (2d Cir. 1985).

[18] *See* Elizabeth Goitein, *The Ninth Circuit's Constitutional Detour in Mohamud*, JUST SEC. (Dec. 8, 2016). https://www.justsecurity.org/35411/ninth-circuits-constitutional-detour-mohamud/. The rulings are particularly inapt because Section 702 minimization procedures present little or no barrier to collection, and the back-end protections on retention and use are significantly weaker than those that apply in the Title III context. *See* Brief for Appellant at Argument I, *In re* Sealed Case, 310 F.3d 717 (FISA Ct. Rev. 2002) (No. 02-001) (noting that "FISA's minimization standards are more generous than those in Title III").

[19] Riley v. California, 134 S. Ct. 2473, 2488 (2014).

[20] United States v. Mohamud, No. 3:10-cr-00475, 2014 WL 2866749 (D. Or. June 24, 2014), *aff'd on other grounds*, 843 F.3d 420 (9th Cir. 2016).

stating that it applies even if the target is an American and even if the primary purpose of collection has no relation to foreign intelligence.[21]

In the era before FISA, however, several federal courts of appeal had the opportunity to review foreign intelligence surveillance, and they articulated a much narrower version of the exception.[22] They held that it applies only if the target is a foreign power or agent thereof, and only if the acquisition of foreign intelligence is the primary purpose of the surveillance. They also emphasized the importance of close judicial scrutiny (albeit after-the-fact) in cases where the target challenges the surveillance. While these cases addressed surveillance activities that differed in many respects from Section 702, it is clear that Section 702 surveillance would not pass constitutional muster under the standards they articulated.

A detailed analysis of the case law is beyond the scope of this testimony, but the Brennan Center's report, *What Went Wrong With the FISA Court*, engages in such an analysis and explains why the foreign intelligence exception does not justify Section 702 surveillance in its current form.[23]

C. The Reasonableness Test

Even if a foreign intelligence exception applied, the surveillance would still have to be "reasonable" under the Fourth Amendment. The "reasonableness" inquiry entails weighing the government's interests against the intrusion on privacy.[24]

In undertaking this analysis, courts generally accept that the government's interest in protecting national security is of the highest order – as it certainly is. But to determine the reasonableness of a surveillance scheme, one must also ask whether it goes further than necessary to accomplish the desired end. For instance, how does it further national security to allow the targeting of foreigners who have no known or suspected affiliation with foreign governments, factions, or terrorist groups? How does it further national security to permit the FBI to search for Americans' communications to use in prosecutions having nothing to do with national security?[25]

Moreover, in assessing the impact on privacy rights, the FISA Court has focused on the protections offered to Americans by minimization procedures.[26] As discussed below, however, these protections fall short in a number of significant respects. On their face, they allow Americans' communications to be retained, disseminated, and used in a wide range of circumstances.

---

[21] *See, e.g.*, *In re Directives*, 551 F.3d 1004; *In re* DNI/AG Certification [REDACTED], No. 702(i)-08-01 (FISA Ct. Sept. 4, 2008).
[22] *See, e.g.*, United States v. Truong Dinh Hung, 629 F.2d 908, 913 (4th Cir. 1980); United States v. Brown, 484 F.2d 418, 426 (5th Cir. 1973); United States v. Butenko, 494 F.2d 593, 604-05 (3rd Cir. 1974) (en banc); United States v. Buck, 548 F.2d 871, 875 (9th Cir. 1977).
[23] GOITEIN & PATEL, *supra* note 2, at 11-12, 35-43.
[24] Maryland v. King, 133 S. Ct. 1958, 1970 (2013).
[25] *See infra* Part V.
[26] *In re Directives*, 551 F.3d at 1015.

III. Risks and Harms of Mass Data Collection

Constitutional concerns aside, the mass collection and storage of communications that include sensitive information about Americans carries with it significant risks and harms, which must be considered in evaluating what the appropriate scope of surveillance should be.

A. Risk of Abuse or Mishandling of Data

The substantive legal restrictions on collecting information about Americans are looser than they have been since before 1978. At the same time, the amount of data available to the government and the capacity to store and analyze that data are orders of magnitude greater than they were during the period of J. Edgar Hoover's worst excesses. History teaches us that this combination is an extraordinarily dangerous one.

To date, there is only limited evidence of intentional abuse of Section 702 authorities.[27] There have, however, been multiple significant instances of non-compliance by the NSA with FISA Court orders. Notably, these include cases in which the NSA did not detect the non-compliance for years, and the agency's overseers had no way to uncover the incidents in the meantime. Given that these incidents went unreported for years even when the agency was *not* trying to conceal them, it is not clear how overseers would learn about intentional abuses that agency officials were making every effort to hide. In other words, regardless of whether intentional abuse is happening today, the *potential* for abuse to take place – and to go undiscovered for long periods of time – is clearly present.

Inadvertent failures to adhere to privacy protections are a concern in their own right. On multiple occasions in the past decade, the FISA Court has had occasion to rebuke the NSA for repeated, significant, and sometimes systemic failures to comply with court orders. These failures took place under multiple foreign intelligence collection authorities (including Section 702) and at all points of the programs: collection, dissemination, and retention. It is instructive to review some of the Court's comments in these cases. The following statements are excerpted from four opinions:

- "In summary, since January 15, 2009, it has finally come to light that the FISC's authorizations of this vast [Section 215 telephony metadata] collection program have been premised on a flawed depiction of how the NSA uses [the] metadata. This misperception by the FISC existed from the inception its authorized collection in May 2006, buttressed by repeated inaccurate statements made in the government's submissions, and despite a government-devised and Court-mandated oversight regime. The minimization procedures proposed by the government in each successive application and approved and adopted as binding by the orders of the FISC have been so frequently

[27] *See, e.g.*, Letter from Dr. George Ellard, Inspector Gen., Nat'l Sec. Agency, to Sen. Charles E. Grassley (Sept. 11, 2013), *available at* http://www.privacylives.com/wp-content/uploads/2013/09/09262013-NSA-Surveillance-09-11-13-response-from-IG-to-intentional-misuse-of-NSA-authority.pdf (detailing 12 instances of intentional abuse of NSA bulk surveillance data, most involving employees searching for information on their romantic partners).

and systemically violated that it can fairly be said that this critical element of the overall [bulk collection] regime has never functioned effectively."[28]

- "The government has compounded its non-compliance with the Court's orders by repeatedly submitting inaccurate descriptions . . . to the FISC."[29]
- "[T]he NSA continues to uncover examples of systematic noncompliance."[30]
- "Under these circumstances, no one inside or outside of the NSA can represent with adequate certainty whether the NSA is complying with those procedures."[31]
- "[U]ntil this end-to-end review is completed, the Court sees little reason to believe that the most recent discovery of a systemic, ongoing violation . . . will be the last."[32]
- "The Court is troubled that the government's revelations regarding NSA's acquisition of Internet transactions mark the third instance in less than three years in which the government has disclosed a substantial misrepresentation regarding the scope of a major collection program."[33]
- "The current application [for pen register/trap and trace data] . . . raises issues that are closely related to serious compliance problems that have characterized the government's implementation of prior FISA orders."[34]
- "As far as can be ascertained, the requirement was simply ignored."[35]
- "Notwithstanding this and many similar prior representations, there in fact had been systematic overcollection since [redacted]. . . . This overcollection . . . had occurred continuously since the initial authorization . . . ."[36]
- "The government has provided no comprehensive explanation of how so substantial an overcollection occurred."[37]
- "[G]iven the duration of this problem, the oversight measures ostensibly taken since [redacted] to detect overcollection, and the extraordinary fact that the NSA's end-to-end review overlooked unauthorized acquisitions that were documented in virtually every record of what was acquired, it must be added that those responsible for conducting oversight at NSA failed to do so effectively."[38]
- "The history of material misstatements in prior applications and non-compliance with prior orders gives the Court pause before approving such an expanded collection. The government's poor track record with bulk PR/TT acquisition…presents threshold concerns about whether implementation will conform with, or exceed, what the government represents and the Court may approve."[39]
- "As noted above, NSA's record of compliance with these rules has been poor. Most notably, NSA generally disregarded the special rules for disseminating United States

---

[28] *In re* Production of Tangible Things from [Redacted], No. BR 08-13, at 10-11 (FISA Ct. Mar. 2, 2009).
[29] *Id.* at 6.
[30] *Id.* at 10.
[31] *Id.* at 15.
[32] *Id.* at 16.
[33] [Redacted], 2011 WL 10945618, at *5 n. 14 (FISA Ct. Oct. 3, 2011).
[34] [Redacted], Docket No. PR/TT [Redacted], at 4 (FISA Ct. [Redacted]) *available at* https://www.dni.gov/files/documents/1118/CLEANEDPRTT%202.pdf.
[35] *Id.* at 19.
[36] *Id.* at 20.
[37] *Id.* at 21.
[38] *Id.* at 22.
[39] *Id.* at 77.

person information outside of NSA until it was ordered to report such disseminations and certify to the FISC that the required approval had been obtained… The government has provided no meaningful explanation why these violations occurred, but it seems likely that widespread ignorance of the rules was a contributing factor."[40]

- "Given NSA's longstanding and pervasive violations of the prior orders in this matter, the Court believes that it would be acting well within its discretion in precluding the government from accessing or using such information."[41]
- "[The] cases in which the FBI had not established the required review teams seemed to represent a potentially significant rate of non-compliance."[42]
- "The Court was extremely concerned about these additional instances of non-compliance."[43]
- "Perhaps more disturbing and disappointing than the NSA's failure to purge this information for more than four years, was the government's failure to convey to the Court explicitly during that time that the NSA was continuing to retain this information . . . ."[44]

It is unclear whether these failures occurred because the NSA was not putting sufficient effort into compliance, because the NSA lacked the technical capability to ensure consistent compliance, or for some other reason. Whatever the explanation, the fact that the agency's many failures to honor privacy protections were inadvertent is of limited comfort when the NSA is asking Congress and the American public to entrust it with extensive amounts of private data.

Moreover, the fact that little evidence of intentional abuse has emerged to date is not a cause for complacency. Government insiders have made reference to a "culture of compliance" and professionalism that emerged in the decades following the Church Committee's investigation.[45] But organizational cultures change, and are highly influenced by leadership. There is simply no guarantee that the degree of institutional self-restraint exercised in the past will continue indefinitely.

In this vein, it is significant that some intelligence experts who until recently defended the wide discretion permitted by Section 702 have seemingly revisited their conclusions in light of today's tumultuous and uncertain political landscape. Matthew Olsen, who served as NSA General Counsel and the Director of the National Counterterrorism Center, was a strong supporter of the FISA Amendments Act when it was being debated in 2008 and has often testified on its behalf.[46] At a recent public conference, however, he stated: "I fought hard . . . for

---

[40] *Id.* at 95.
[41] *Id.* at 115.
[42] [Redacted], at 48-49 (FISA Ct. Nov. 6, 2015), *available at* www.dni.gov%2Ffiles%2Fdocuments%2F20151106-702Mem_Opinion_Order_for_Public_Release.pdf&t=MDM3MGZmYjY1ZWQ5YjUyMTQ5ZjQ1ZTA0ZDExNjY2NWU0ZTE1ZWJlNSxaRjRxYlRaQg%3D%3D.
[43] *Id.* at 50.
[44] *Id.* at 58.
[45] See Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GEO.WASH. L. REV. 1306, 1326 n.135 (2004).
[46] *See, e.g., Oversight and Reauthorization of the FISA Amendments Act: The Balance between National Security, Privacy, and Civil Liberties: Hearing Before the S. Comm. on the Judiciary,* 114th Cong. (2016) (statement of Matthew G. Olsen, Former Director, National Counterterrorism Center) [hereinafter Olsen Statement].

increasing information sharing… [and] for the modernization of FISA. . . . As I fought for these changes, I did not bargain on [the current political environment]. That was beyond my ability to imagine . . . [T]his is a time of . . . soul-searching for me."[47]

B. Chilling Effect

When Americans are aware that intelligence agencies are collecting large amounts of their data (and not just the data of suspected criminals and terrorists), it creates a measurable chilling effect on free expression and communication. After Edward Snowden's revelations in June 2013, an analysis of Google Trends data showed a significant five percent drop in U.S.-based searches for government-sensitive terms (e.g., "dirty bomb" or "CIA"). A control list of popular search terms or other types of sensitive terms (such as "abortion") did not show the same change.[48] In 2013, PEN America surveyed 528 American writers to learn how the disclosures affected their behavior. Twenty-eight percent reported curtailing social media activities; 24 percent avoided certain topics by phone or email; 16 percent chose not to write or speak on a certain topic; and 16 percent avoided Internet searches or website visits on controversial or suspicious topics.[49] These kinds of self-censorship are inimical to the robust exchange of ideas necessary for a healthy democracy.

The impact of overbroad surveillance has been particularly acute in Muslim American communities. According to one study, after the Associated Press reported on the New York City Police Department's surveillance activities, Muslims reported a decline in mosque attendance and Muslim Student Association participation, as well as a marked reticence to speak about political matters in public places or to welcome newcomers into the community.[50] Fear of surveillance, and the possibility that religious or political discussions could be misconstrued or misunderstood, has measurably impeded these communities' ability to freely practice their faith or even to participate fully in civic life.

C. Risk of Data Theft

Any massive government database containing sensitive information about Americans also raises concerns about data theft. The disastrous 2015 attack on the Office of Personnel Management's database, in which personal data concerning more than 21 million current and former federal employees was stolen (ostensibly by the Chinese government), illustrated how vulnerable government databases are.[51] A few months later, hackers published contact

---

[47] *Intelligence Under a Trump Administration*, Panel Discussion at 2016 Cato Surveillance Conference, CATO INSTITUTE, at 47:20 (Dec. 14, 2016), https://www.cato.org/multimedia/events/2016-cato-surveillance-conference-panel-intelligence-under-trump-administration.

[48] Alex Marthews & Catherine Tucker, *Government Surveillance and Internet Search Behavior* (Apr. 29, 2015), *available at* http://dx.doi.org/10.2139/ssrn.2412564.

[49] Lee Rainie & Mary Madden, *Americans' Privacy Strategies Post-Snowden*, PEW RESEARCH CTR (Mar. 16, 2015), http://www.pewinternet.org/2015/03/16/americans-privacy-strategies-post-snowden/.

[50] *See generally* MUSLIM AMERICAN CIVIL LIBERTIES COALITION (MACLC) ET AL., MAPPING MUSLIMS: NYPD SPYING AND ITS IMPACT ON AMERICAN MUSLIMS (2013), *available at* http://www.law.cuny.edu/academics/clinics/immigration/clear/Mapping-Muslims.pdf.

[51] Kaveh Waddell & Dustin Volz, *OPM Announces More Than 21 Million Victims Affected by Second Data Breach*, ATLANTIC (July 9, 2015). http://www.theatlantic.com/politics/archive/2015/07/opm-announces-more-than-21-million-affected-by-second-data-breach/458475/.

information for 20,000 FBI employees and 10,000 Department of Homeland Security employees that they may have obtained by hacking into a Department of Justice database.[52] The broad scope of Section 702 data, and the possibility that it could include a wealth of valuable foreign intelligence information, makes it an attractive target for hacking. Its inclusion of large amounts of information about presumptively innocent Americans significantly increases the harm that would be caused by such an event.

D. Economic Consequences

Another important concern is the negative impact of Section 702 collection on the U.S. technology industry. After Snowden's disclosures revealed the extent of NSA collection, American technology companies reported declining sales overseas and lost business opportunities. In a survey of 300 British and Canadian businesses, 25 percent of respondents indicated they were moving their data outside of the U.S.[53] An August 2013 study by the Information Technology and Innovation Foundation estimated that the revelations could cost the American cloud computing industry $22 to $35 billion over the coming years, representing a 10-20% loss of the foreign market share to European or Asian competitors.[54] Another analyst found this estimate to be low, and predicted a loss to U.S. companies as high as $180 billion.[55]

The economic news went from bad to worse in late 2015, when the Court of Justice of the European Union (CJEU) invalidated the "Safe Harbor" agreement – a 2000 decision of the European Commission allowing the transfer of personal data from the European Union (EU) to the United States, based on the premise that the U.S. met certain EU-law requirements about the handling of that information. The court held that EU law requires U.S. companies to give the data a level of protection that is essentially equivalent to the protections under EU law, including the Charter of Fundamental Rights of the EU – akin to an EU bill of rights. Under this standard, the court found that the European Commission had failed to ensure that EU citizens' data was sufficiently protected within the U.S. While the court did not make express findings about Section 702, the law unquestionably loomed large in the court's analysis, as the authority it confers is inconsistent with many of the essential rights and principles the court described. For instance, upstream surveillance is clearly implicated by the CJEU's conclusion that "generalized" access to the content of electronic communications compromises the essence of the right to privacy.[56]

---

[52] Mary Kay Mallonnee, *Hackers Publish Contact Info of 20,000 FBI Employees*, CNN (Feb. 8, 2016), http://www.cnn.com/2016/02/08/politics/hackers-fbi-employee-info/.

[53] DANIELLE KEHL, ET. AL, OPEN TECHNOLOGY INSTITUTE, SURVEILLANCE COSTS: THE NSA'S IMPACT ON THE ECONOMY, INTERNET FREEDOM & CYBERSECURITY 8 (2014), https://static.newamerica.org/attachments/534-surveillance-costs-the-nsas-impact-on-the-economy-internet-freedom-cybersecurity/Surveillance_Costs_Final.pdf.

[54] DANIEL CASTRO, INFORMATION TECHNOLOGY AND INNOVATION FOUNDATION, "HOW MUCH WILL PRISM COST THE US CLOUD COMPUTING INDUSTRY?" (Aug. 5, 2013), http://www.itif.org/publications/how-much-will-prism-cost-us-cloud-computing-industry.

[55] James Staten, *The Cost of PRISM Will Be Larger Than ITIF Projects*, FORRESTER (Aug. 14, 2013), http://blogs.forrester.com/james_staten/13-08-14-the_cost_of_prism_will_be_larger_than_itif_projects.

[56] *See* Case C-362/14, Schrems v. Data Protection Commissioner, ECLI:EU:C:2015:650 (Oct. 6, 2015), *available at* http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&doclang=en; *see also* Sarah St. Vincent, *Making Privacy a Reality: The Safe Harbor Judgment and Its Consequences for US Surveillance*, CENTER FOR DEMOCRACY & TECHNOLOGY (Oct. 26, 2015), https://cdt.org/blog/making-privacy-a-reality-the-safe-harbor-

Although the U.S. and the European Commission have devised a new arrangement, known as the "Privacy Shield," legal challenges to that agreement are underway[57] – and recent developments have given a boost to these challenges. In particular, some of the protections U.S. officials had cited to assuage concerns about the breadth of Section 702 and other U.S. surveillance programs have been, or may soon be, eroded. The Privacy and Civil Liberties Oversight Board has lost its chairman and three other members, and is effectively dormant. A recent executive order issued by President Trump removes Privacy Act protections for foreigners. The current CIA director previously proposed revoking a directive issued by President Obama that extended some protections to foreigners' data obtained under foreign intelligence programs.[58]

In the absence of reforms to Section 702 and other surveillance authorities, it appears likely that the Privacy Shield will ultimately be invalidated by the CJEU or potentially even by the European Commission itself (which can suspend the arrangement unilaterally). Experts believe this would deal a massive economic blow to U.S. companies and could undermine the very structure of the Internet, which requires free data flow across borders. In the meantime, the legal limbo in which U.S. companies find themselves constrains their ability to pursue business opportunities in Europe.

E. Potential National Security Harms

Last but clearly not least, there is a risk to national security in acquiring too much data. While computers can glean relationships and flag anomalies, they cannot replace human analysis, and human beings have limited capacity. When they are presented with an excess of data, real threats can get lost in the noise. This is not merely a theoretical concern. After the intelligence community failed to intercept the so-called "underwear bomber" (the suicide bomber who nearly brought down a plane headed to Detroit on Christmas Day 2009), an official White House review observed that a significant amount of critical information was available to the intelligence agencies but was "embedded in a large volume of other data."[59] Similarly, the independent investigation of the FBI's role in the shootings by U.S. Army Major Nidal Hasan at Fort Hood concluded that the "crushing volume" of information was one of the factors that hampered accurate analysis prior to the attack.[60]

---

judgment-and-its-consequences-for-us-surveillance-reform/ (describing the relationship between the CJEU's holding and Section 702 surveillance).

[57] *See* Reuters, *French Privacy Groups Challenge the EU's Personal Data Pact with U.S.*, FORTUNE (Nov. 2, 2016), http://fortune.com/2016/11/02/privacy-shield-pact-challenge/.

[58] *See* Letter from Fanny Hidvégi, European Policy Manager, & Amie Stepanovich, U.S. Policy Manager, Access Now, for Vera Jourová, Commissioner, European Commission, & Claude Moraes, Member, European Parliament, re: Impact of new U.S. policies and regulatory frameworks on the privacy rights of users in Europe (Feb. 8, 2017), *available at* https://www.accessnow.org/cms/assets/uploads/2017/02/Letter-to-Jourova.pdf.

[59] THE WHITE HOUSE, SUMMARY OF THE WHITE HOUSE REVIEW OF THE DECEMBER 25, 2009 ATTEMPTED TERRORIST ATTACK 3, *available at* http://www.whitehouse.gov/sites/default/files/summary_of_wh_review_12-25-09.pdf.

[60] *Lessons from Fort Hood: Improving Our Ability to Connect the Dots: Hearing Before the Subcomm. on Oversight, Investigations, and Mgmt. of the H. Comm. on Homeland Security*, 112th Cong. 2 (2012) (statement of Douglas E. Winter, Deputy Chair, William H. Webster Commission on the Fed. Bureau of Investigation, Counterterrorism Intelligence, and the Events at Fort Hood, Texas on November 5, 2009).

Whatever threat information may exist amidst the 250 million Internet communications acquired yearly under Section 702, there is surely a large amount of chaff. Because this may make it more difficult to find the threats, it is important for lawmakers to examine whether the current scope of Section 702 collection may be too broad from a security standpoint as well as a privacy one.

IV. Minimization and Its Loopholes

Legal and policy defenses of Section 702 surveillance rely heavily on the existence of minimization procedures to mitigate the effects of "incidental" collection. The concept behind minimization is fairly simple: The interception of Americans' communications when targeting foreigners is inevitable, but because such interception ordinarily would require a warrant or individual FISA order, incidentally collected U.S. person information generally should not be kept, shared, or used, subject to narrow exceptions.

The statutory language, however, is much more complex. It requires the government to adopt minimization procedures, which it defines as procedures "that are reasonably designed . . . to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information."[61] The statute also prohibits disseminating non-foreign intelligence information in a way that identifies U.S. persons unless their identity is necessary to understand foreign intelligence information or assess its importance. The one caveat is that the procedures must "allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes."[62]

The lack of specificity in this definition, and the tension between its general rule and its caveat, has allowed the government to craft rules that are permissive and contain multiple exceptions. To begin with, the NSA may share raw data with the FBI and CIA.[63] All three agencies generally may keep unreviewed raw data – including data about U.S. persons – for five years after the certification expires;[64] they also can seek extensions from a high-level official,[65]

---

[61] 50 U.S.C. § 1801(h)(1).

[62] 50 U.S.C. § 1801(h)(3).

[63] LORETTA LYNCH, U.S. DEP'T OF JUSTICE, MINIMIZATION PROCEDURES USED BY THE NATIONAL SECURITY AGENCY IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED § 6(c) (2015) [hereinafter NSA 702 MINIMIZATION PROCEDURES], *available at* https://www.dni.gov/files/documents/2015NSAMinimizationProcedures_Redacted.pdf.

[64] *Id.* at § 3(c)(1) (2015) (although the retention period for communications obtained through upstream collection is two years, as specified in section 3(c)(2)); LORETTA LYNCH, U.S. DEP'T OF JUSTICE, MINIMIZATION PROCEDURES USED BY THE FEDERAL BUREAU OF INVESTIGATION IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED § III.G.1.a (2015) [hereinafter FBI 702 MINIMIZATION PROCEDURES], *available at* https://www.dni.gov/files/documents/2015FBIMinimization_Procedures.pdf; LORETTA LYNCH, U.S. DEP'T OF JUSTICE, MINIMIZATION PROCEDURES USED BY THE CENTRAL INTELLIGENCE AGENCY IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED § 2 (2015) [hereinafter CIA 702 MINIMIZATION PROCEDURES], *available at* https://www.dni.gov/files/documents/2015CIAMinimizationProcedures_Redacted.pdf.

and the 5-year limit does not apply to encrypted communications (which are becoming increasingly common among ordinary users of mobile devices) or communications "reasonably believed to contain secret meaning."[66] The agencies may keep indefinitely any U.S. person information that has foreign intelligence value or is evidence of a crime.[67]

If the NSA discovers U.S. person data that has no foreign intelligence value and contains no evidence of a crime, the agency is supposed to purge the data.[68] The NSA, however, interprets this requirement to apply only if the NSA analyst determines "not only that a communication is not currently of foreign intelligence value to him or her, but also would not be of foreign intelligence value to any other present or future foreign intelligence need."[69] This is an impossibly high bar, and so, "in practice, this requirement rarely results in actual purging of data."[70]

The FBI and the CIA have no affirmative requirement to purge irrelevant U.S. person data on detection, relying instead on age-off requirements. Moreover, if the FBI reviews information containing U.S. person information and makes *no determination* regarding whether it is foreign intelligence information or evidence of a crime, the 5-year limit evaporates, and the FBI may keep the data for a longer period of time that remains classified.[71]

If any of the three agencies – all of which have access to raw data – disseminate information to other agencies, they must first obscure the identity of the U.S. person; but once again, there are several exceptions to this rule. For instance, the agencies need not obscure the U.S. person's identity if it is necessary to understand or assess foreign intelligence or if the communication contains evidence of a crime.[72]

In short, the NSA routinely shares raw Section 702 data with the FBI and CIA; and the agencies' minimization procedures suggest that U.S. person information is almost always kept for at least five years and, in many circumstances, much longer. The sharing and retention of U.S. person information are not unrestricted, but it is a stretch to say that they are "minimized" under any common sense understanding of the term.

---

[65] PCLOB 702 REPORT, *supra* note 5, at 60.
[66] NSA 702 MINIMIZATION PROCEDURES, *supra* note 63, at § 6(a)(1)(a); CIA 702 MINIMIZATION PROCEDURES, *supra* note 64, at § 3.c.
[67] NSA 702 MINIMIZATION PROCEDURES, *supra* note 63, at § 6(a); FBI 702 MINIMIZATION PROCEDURES, *supra* note 64, at § III.G; CIA 702 MINIMIZATION PROCEDURES, *supra* note 64, at §§ 3.a, 7.d.
[68] NSA 702 MINIMIZATION PROCEDURES, *supra* note 63, at §§ 3(b)(1), 3(c).
[69] PCLOB 702 REPORT, *supra* note 5, at 62.
[70] *Id.*
[71] FBI 702 MINIMIZATION PROCEDURES, *supra* note 64, at § III.G.1.b.
[72] *Id.* at § V.A-B; NSA 702 MINIMIZATION PROCEDURES, *supra* note 63, at § 6(b); CIA 702 MINIMIZATION PROCEDURES, *supra* note 64, at §§ 5, 7.d.

V. Back Door Searches

Perhaps the most problematic aspect of the minimization procedures is that they allow all three agencies to query Section 702 data using U.S. person identifiers, with the express goal of retrieving and analyzing Americans' communications.[73]

If the government wishes to obtain an American's communications for foreign intelligence purposes, it must secure an individual court order from the FISA Court after demonstrating that the target is an agent of a foreign power. If the government wishes to obtain an American's communications for law enforcement purposes, it must get a warrant from a neutral magistrate. To ensure that Section 702 is not used to avoid these requirements, the statute contains a prohibition on "reverse targeting" – i.e., targeting a foreigner overseas when the government's intent is to target "a particular, known person reasonably believed to be in the United States." Before conducting Section 702 surveillance, the government must certify that it does *not* intend to target particular, known Americans.

And yet, immediately upon obtaining the data, all three agencies may sort through it looking for the communications of particular, known Americans – the very people in whom the government just disclaimed any interest. Worse, even though the FBI would be required to obtain a warrant in order to access Americans' communications absent a significant foreign intelligence purpose, the FBI may search the Section 702 data for Americans' communications to use in criminal proceedings having no foreign intelligence dimensions whatsoever.[74] This is a bait and switch that is utterly inconsistent with the spirit, if not the letter, of the prohibition on reverse targeting. It also creates a massive end run around the Fourth Amendment's warrant requirement.

Some have defended these "back door searches," claiming that as long as information is lawfully acquired, agencies may use the information for any legitimate government purpose. This argument ignores Congress's command to agencies to "minimize" information about U.S. persons. The very meaning of "minimization" is that agencies may *not* use the information for any purpose they wish. Minimization is a constitutional requirement as well as a statutory one: as Judge Bates of the FISA Court has observed, "[T]he procedures governing retention, use, and dissemination bear on the reasonableness under the Fourth Amendment of a program for collecting foreign intelligence information."[75]

---

[73] NSA 702 MINIMIZATION PROCEDURES, *supra* note 63, at § 3(b)(5); FBI 702 MINIMIZATION PROCEDURES, *supra* note 64, at § III.D; CIA 702 MINIMIZATION PROCEDURES, *supra* note 64, at § 4.

[74] ROBERT S. LITT, ODNI, PRIVACY, TECHNOLOGY AND NATIONAL SECURITY: AN OVERVIEW OF INTELLIGENCE COLLECTION (July 18, 2013). https://www.dni.gov/index.php/newsroom/speeches-and-interviews/195-speeches-interviews-2013/896-privacy,-technology-and-national-security-an-overview-of-intelligence-collection.

[75] [Redacted], 2011 WL 10945618, at *27 (FISA Ct. Oct. 3, 2011). In cases involving the foreign intelligence exception to the warrant requirement, the reasonableness of a surveillance scheme turns on weighing the government's national security interest against the privacy intrusion. While the surveillance scheme should be evaluated as a whole, it is difficult to see how any scheme could pass the reasonableness test if a significant component of the scheme were not justified by any national security interest. This is one of several errors, in my view, in the FISA Court's 2015 decision upholding the constitutionality of back door searches. *See* Elizabeth Goitein, *The FBI's Warrantless Surveillance Back Door Just Opened a Little Wider*, JUST SEC. (Apr. 21, 2016), https://www.justsecurity.org/30699/fbis-warrantless-surveillance-door-opened-wider/.

Indeed, restrictions on searches of lawfully obtained data are the constitutional norm, not the exception. In executing warrants to search computers, the government routinely seizes and/or copies entire hard drives. However, agents may only conduct searches reasonably designed to retrieve those documents or files containing the evidence specified in the warrant.[76] The fact that the government lawfully obtained and is in possession of the computer's contents does not give it license to conduct any search it wishes; that would violate the terms on which the government obtained the computer's contents in the first place.

The same principle holds true in the analog world. When the police obtain a warrant to search a house for a murder weapon, they may enter the house and, in appropriate cases, search every room. But after they find (or fail to find) the murder weapon, they are not allowed to continue searching for other items they may have some interest in, simply because they are now in the house. Their entrance into the house was legal, but that does not entitle them to search for anything inside it. That would be exceeding the terms accompanying their initial access to the house.

Under Section 702, the terms on which the government is authorized to collect data *without* a warrant include a limitation on whom the government may target – i.e., the government may only target foreigners overseas. To obtain access to the data on those terms and then search for Americans' data is the equivalent of seizing a computer to search for child pornography and then searching for evidence of tax fraud, or obtaining access to a house to search for a murder weapon and then conducting a search for drugs.

Compounding the constitutional harm, the government has not fully and consistently complied with its statutory and constitutional obligation to notify criminal defendants when it uses evidence "obtained or derived from" Section 702 surveillance. Before 2013, the government interpreted "obtained or derived from" so narrowly that it notified no one. In the three and a half years since the government's approach reportedly changed,[77] the government has provided notification in only eight known cases, even though the Privacy and Civil Liberties Oversight Board (PCLOB) reports that the FBI searches Section 702 every time it conducts a national security investigation[78] and there have been several hundred terrorism and national security convictions during this time.[79] There is reason for concern that the government is avoiding its notification requirements by engaging in "parallel construction" – i.e., recreating the Section 702 evidence using less controversial means.[80] Attorneys have asked the Department of Justice to

---

[76] *See, e.g.*, United States v. Ganias, 755 F.3d 125 (2nd Cir. 2014), *rev'd en banc on other grounds*, 824 F.3d 199 (2nd Cir. 2016).

[77] For more background, see Patrick C. Toomey, *Why Aren't Criminal Defendants Getting Notice of Section 702 Surveillance — Again?*, JUST SEC. (Dec. 11, 2015), https://www.justsecurity.org/28256/arent-criminal-defendants-notice-section-702-surveillance-again.

[78] PCLOB 702 REPORT, *supra* note 5, at 59.

[79] DEP'T OF JUSTICE, UNITED STATES ATTORNEYS' ANNUAL STATISTICAL REPORT FISCAL YEAR 2015 at 14; DEP'T OF JUSTICE, UNITED STATES ATTORNEYS' ANNUAL STATISTICAL REPORT FISCAL YEAR 2014 at 12; DEP'T OF JUSTICE, UNITED STATES ATTORNEYS' ANNUAL STATISTICAL REPORT FISCAL YEAR 2013 at 60.

[80] *See* Toomey, *supra* note 69; John Shiffman and Kristina Cooke, *Exclusive: U.S. Directs Agents to Cover Up Program Used to Investigate Americans*, REUTERS (Aug. 5, 2013, 3:25 PM), http://www.reuters.com/article/us-dea-sod-idUSBRE97409R20130805#X7BeCQSb0GrEDTJX.97.

share its policies for determining when information is considered to be "derived from" Section 702, but the Department refuses to provide them.

Importantly, opposition to warrantless searches for U.S. person information is not a call to re-build the barriers to cooperation among agencies often attributed to "the wall." Threat information, including threat information that focuses on U.S. persons, can and should be shared among agencies when identified, and the agencies should work together as necessary in addressing the threat. What the Fourth Amendment cannot tolerate is the government collecting information without a warrant with the intent of mining it for use in ordinary criminal cases against Americans. That is why President Obama's Review Group on Intelligence and Communications Technologies – a five-person panel including a former acting director of the CIA (Michael J. Morell) and chief counterterrorism advisor to President George W. Bush (Richard A. Clarke) – unanimously recommended closing the "back door search" loophole by prohibiting searches for Americans' communications without a warrant.[81]

VI. Foreign Nationals and Human Rights Risks

Section 702 surveillance also raises concerns about the privacy and human rights of foreign nationals who are not foreign powers, agents of foreign powers, or affiliated with terrorism. While the Fourth Amendment might not apply to these individuals, the right to privacy is a fundamental human right recognized under international law – including treaties, such as the International Covenant on Civil and Political Rights, that the U.S. has signed. In Presidential Policy Directive 28 (PPD-28), President Obama acknowledged that "all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and . . . all persons have legitimate privacy interests in the handling of their personal information."[82]

PPD-28 requires agencies to extend certain privacy protections to foreign nationals when conducting electronic surveillance. Most notably, personal information of non-U.S. persons may be retained or disseminated only if retention and sharing would be permitted for "comparable information concerning U.S. persons."[83] This is a significant change, but several factors limit its actual and potential impact.

Most notably, the future viability of PPD-28 is uncertain, given that President Trump already has rescinded several of President Obama's orders and CIA Director Mike Pompeo, when he served in Congress, argued that PPD-28 should be revoked.[84] Additionally, even if PPD-28 remains in place, the directive does not prevent the *acquisition* of information about foreign nationals who pose no threat to the United States. Finally, the limits on *retention and sharing* of U.S. person information are not particularly strict to begin with, and it remains to be

---

[81] *See* PRESIDENT'S REVIEW GRP. ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES, LIBERTY AND SECURITY IN A CHANGING WORLD 29 (2013), *available at* http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

[82] EXEC. OFFICE OF THE PRESIDENT, PRESIDENTIAL POLICY DIRECTIVE/PPD-28 (2014), *available at* http://www.lawfareblog.com/wp-content/uploads/2014/01/2014sigint.mem_.ppd_.rel_.pdf.

[83] *Id.*at § 4(a)(i).

[84] *See* Mike Pompeo & David B. Rivkin Jr., *Time for a Rigorous National Debate About Surveillance*, WALL ST. J. (Jan. 3, 2016). https://www.wsj.com/articles/time-for-a-rigorous-national-debate-about-surveillance-1451856106.

seen whether and how the agencies incorporated PPD-28's requirement of "comparability" in their 2015 minimization procedures (which have not been declassified).

A particular concern relates to the sharing of Section 702 information with foreign governments. Agencies have significant leeway to share foreign intelligence information, as long as the sharing is consistent with U.S. law, clearly in the national interest, and "intended for a specific purpose and generally limited in duration."[85] Although the agency should have "confidence" that the information "is not likely to be used by the recipient in an unlawful manner or in a manner harmful to U.S. interests,"[86] there is no express requirement or mechanism to ensure that governments with poor or spotty human rights records will not use the information to facilitate human rights violations – for instance, to harass or persecute journalists, political dissidents, human rights activists, and other vulnerable groups whose communications may have been caught up in the Section 702 collection.[87]

VII. Must We Leave Section 702 in Its Current Form?

Having discussed the concerns surrounding Section 702 surveillance, it is important to address the arguments that have been put forward for its necessity. These arguments have varying degrees of merit, but none of them forecloses the possibility of reforms.

A. Restoring FISA's Original Intent?

Executive branch officials have argued that Section 702 was necessary to restore the original intent behind FISA, which was being subverted by changes in communications technology. These officials note that FISA in 1978 required the government to obtain an individual court order when collecting any communications involving Americans that traveled by wire, but required an individual court order to obtain satellite communications only when all of the communicants were inside the U.S. Asserting that "'wire' technology was the norm for domestic calls,"[88] while "almost all transoceanic communications into and out of the United States were carried by satellite, which qualified as 'radio' (vs. 'wire') communications,"[89] they infer that Congress intended to require the government to obtain an order when acquiring purely domestic communications, but not when obtaining communications between foreign targets and Americans. This intent was undermined when fiber-optic cables later became the standard method of transmission for international calls.

---

[85] OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, FOREIGN DISCLOSURE AND RELEASE OF CLASSIFIED NATIONAL INTELLIGENCE, ICD 403 § E(1) (Mar. 13, 2013), *available at* http://www.dni.gov/files/documents/ICD/ICD403.pdf.

[86] OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, CRITERIA FOR FOREIGN DISCLOSURE AND RELEASE OF CLASSIFIED NATIONAL INTELLIGENCE, ICPG 403.1 § (D)(2) (Mar. 13, 2013), *available at* http://www.dni.gov/files/documents/ICPG/ICPG403-1.pdf.

[87] *See* AMOS TOH, FAIZA PATEL & ELIZABETH GOITEIN, BRENNAN CTR. FOR JUSTICE, OVERSEAS SURVEILLANCE IN AN INTERCONNECTED WORLD 28-31 (2016), http://www.brennancenter.org/sites/default/files/publications/Overseas_Surveillance_in_an_Interconnected_World.pdf.

[88] Statement of Kenneth L. Wainstein, Partner, Cadwalader, Wickersham & Taft LLP, before the Subcommittee on Crime, Terrorism, and Homeland Security of the House Committee on the Judiciary at 4 (May 31, 2012).

[89] Statement of Kenneth L. Wainstein, Assistant Attorney General, National Security Division, Department of Justice, before the House Permanent Select Committee on Intelligence at 4 (Sept. 6, 2007).

The problem with this theory is two-fold. First, it would have been quite simple for Congress to state that FISA orders were required for purely domestic communications and not for international ones. Instead, Congress produced an elaborate, multi-part definition of "electronic surveillance" that relied on particular technologies rather than the domestic versus international nature of the communication. Second, it is not correct that "almost all" international communications were carried by satellite; the available evidence indicates that one third to one half of international communications were carried by wire.[90]

A more plausible explanation for the original FISA's complex scheme – one with much stronger support in the legislative history – was put forward by David Kris, a former head of the Justice Department's National Security Division. Mr. Kris concluded that Congress intended to require a court order for international wire communications obtained in the U.S., and that the purpose behind its definitional acrobatics was to leave legislation covering surveillance conducted outside the U.S. and NSA satellite surveillance for another day.[91] Although Congress never followed up, the legislative history of FISA made clear that the gaps in the statute's coverage of NSA's operations "should not be viewed as congressional authorization for such activities as they affect the privacy interests of Americans."[92]

A related argument in support of Section 702's necessity is that certain purely foreign-to-foreign communications, which Congress never intended to regulate, now travel through the United States in ways that bring them within FISA's scope. In practice, this appears to be a fairly discrete (albeit thorny) problem that applies to one category of communication: e-mails between foreigners that are stored on U.S. servers.[93] Section 702, however, goes far beyond what would be necessary to solve that problem, as it eliminates the requirement of an individualized court order for the acquisition of any communication between a foreign target and an American.

Moreover, there is a flip side to this issue: changes in technology have also caused certain purely domestic communications to travel *outside* the U.S. in ways that *remove* them from FISA's scope. Purely domestic communications once traveled on copper wires inside the U.S., and FISA thus required a court order to obtain them for foreign intelligence purposes. Today, digital data may be routed anywhere in the world – and U.S. Internet Service Providers may store domestic communications on overseas servers – rendering these communications vulnerable to surveillance under Executive Order 12333, which has far fewer safeguards.[94] Any legislation

---

[90] David Kris, *Modernizing the Foreign Intelligence Surveillance Act* 3 (Brookings Inst., Working Paper, 2007), *available at* http://www.brookings.edu/~/media/research/files/papers/2007/11/15%20nationalsecurity%20kris/1115_nationalsecurity_kris.pdf.

[91] *Id.* at 13-23.

[92] S. REP. NO. 95-701, at 35 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3973, 4004.

[93] FISA regulates three basic types of surveillance: wiretapping, the interception of radio communications, and the "monitoring" of information through other electronic means — which, in 1978, referred primarily to bugging. Although e-mails may be captured in transit by wiretapping or (for e-mails sent wirelessly) interception of radio signals, once they are stored on a server, their acquisition is considered "monitoring." Because FISA regulates "monitoring" within the U.S. regardless of the nationality of the target, stored foreign-to-foreign e-mails come within its ambit. DAVID S. KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS & PROSECUTIONS 2d §§ 7.27, 16.6 (2012).

[94] GOITEIN & PATEL, *supra* note 2, at 19-20; TOH ET AL., *supra* note 87, at 8-10.

that attempts to address the unanticipated inclusion of purely foreign communications should address the unanticipated exclusion of purely domestic communications, as well.

It should also address another way in which technological advances have undermined the protections of FISA. As noted above, FISA governs the acquisition of "wire" communications as long as one of the communicants is inside the United States, but it governs the acquisition of "radio" communications only if the sender and all recipients are inside the United States.[95] In addition, even if a communication travels most of its route by wire, it is considered a "radio" communication if intercepted during a non-wire portion of transmittal.[96] Today, as cell phones are replacing landlines, more and more "wire communications" have a wireless component[97] – allowing the government to acquire an increasing number of international phone calls on U.S. soil outside FISA's legal framework. This unintended exception to FISA's coverage threatens to swallow the rule, unless Congress acts to fix it.

B. Thwarting Terrorist Plots

Executive officials have stated, and the PCLOB and the president's Review Group on Intelligence and Communications Technologies have found, that Section 702 surveillance played a role in detecting and thwarting a number of terrorist plots. That is, after all, the most important function the statute is intended to serve; if it did *not* accomplish this goal, it presumably should go the way of the now-discontinued Section 215 bulk collection program, which, by most reliable reports, added little counterterrorism value.

Whether Section 702 is useful is thus a question of critical importance. It is not, however, the only question that must be answered. There is also the question of whether effective surveillance could be conducted in a manner that entails less intrusion on the privacy of law-abiding Americans and foreigners. Indeed, in the few cases that have been made public – including those of Najibullah Zazi, Khalid Ouazzani, David Headley, Agron Hasbajrami, and Jamshid Muhtorov – it appears that the targets of the Section 702 surveillance were known or suspected to have terrorist affiliations.[98] Intelligence officials have confirmed that this is the norm in cases where Section 702 surveillance has been critical – i.e., that the "typical" such case has involved "narrowly focused surveillance" targeting "a specific foreign individual overseas[,] based on the government's reasonable belief the individual was involved with terrorist activities."[99] Such cases do not support the idea that the NSA needs the authority to target any foreigner overseas and collect all of his communications with Americans.

---

[95] 50 U.S.C. § 1801(f)(2) & (3).
[96] *See* KRIS & WILSON, *supra* note 93, at § 7.6.
[97] Although most wireless communications today do not technically travel via radio waves, the legislative history of FISA indicates that Congress intended to cover a broader range on the electromagnetic spectrum. *See id.* at § 7.7.
[98] *See 2009 Subway Plot*, NEW AMERICA, http://securitydata.newamerica.net/extremists/terror-plot.html?id=1543; *2009 New York Stock Exchange Plot*, NEW AMERICA, http://securitydata.newamerica.net/extremists/terror-plot.html?id=1542; *2009 Jyllands Posten Plot*, NEW AMERICA, http://securitydata.newamerica.net/extremists/terror-plot.html?id=1583; *2011 Agron Hasbajrami*, NEW AMERICA, http://securitydata.newamerica.net/extremists/terror-plot.html?id=1616; *2012 Islamic Jihad Union Support Network*, NEW AMERICA, http://securitydata.newamerica.net/extremists/terror-plot.html?id=1575.
[99] *See* Olsen Statement, *supra* note 46, at 5.

We must also ask whether the costs to our liberties are too high. It is commonly said that if terrorists succeed in undermining our values, they win. But while this notion is often invoked, it is also often forgotten. The United States was founded on a set of core principles, and none of these was more important than the right of the citizens to be free from undue intrusions by the government on their privacy.[100] Our Constitution promises us that law-abiding citizens will be left alone. It is incumbent upon us as a nation to find ways of addressing the terrorist threat that do not betray this promise.

VIII. Who Decides? – The Need for Transparency

Within constitutional bounds set by our nation's courts, it is up to the American people – speaking through their representatives in Congress – to decide how much surveillance is too much. But they cannot do this without sufficient information.

While a significant amount of information about Section 702 has been declassified in recent years, critical information remains unavailable. For instance, the certifications setting forth the categories of foreign intelligence the government seeks to collect – but not the individual targets – have not been released, even in redacted form. Unlike the NSA and the CIA, the FBI does not track or report how many times it uses U.S. person identifiers to query databases containing Section 702 data. The list of crimes for which Section 702 data may be used as evidence has not been disclosed. Nor have the policies governing when evidence used in legal proceedings is considered to be "derived from" Section 702 surveillance. The length of time that the FBI may retain data that has been reviewed but whose value has not been determined remains secret.

Perhaps most strikingly, despite multiple requests from lawmakers dating back several years, the NSA has yet to disclose an estimate of how many Americans' communications are collected under Section 702. The NSA has previously stated that generating an estimate would itself violate Americans' privacy, ostensibly because it might involve reviewing communications that would otherwise not be reviewed. In October of last year, a coalition of more than thirty advocacy groups – including many of the nation's most prominent privacy organizations – sent a letter to the Director of National Intelligence urging that the NSA go forward with producing an estimate.[101] The letter noted that, as long as proper safeguards were in place, the result would be a net gain for privacy.

In April 2016, a bipartisan group of fourteen House Judiciary Committee members sent the DNI a letter making the same request.[102] Eight months later, the members wrote again to memorialize their understanding, in light of interim conversations and briefings, that the DNI would provide the requested estimate "early enough to inform the debate," and with a target date

---

[100] Michael W. Price, *Rethinking Privacy: Fourth Amendment "Papers" and the Third-Party Doctrine*, 8 J. NAT ' L SECURITY L. & POL ' Y 247, 250-64 (2015).
[101] Letter from Brennan Ctr. for Justice, et. al, to James Clapper, Dir. Nat'l Intelligence (Oct. 29, 2015), *available at* https://www.brennancenter.org/sites/default/files/analysis/Coalition_Letter_DNI_Clapper_102915.pdf.
[102] Letter from Rep. John Conyers, Jr., et. al, to James Clapper, Dir. Nat'l Intelligence (Apr. 22, 2016), *available at* https://www.brennancenter.org/sites/default/files/legal-work/Letter_to_Director_Clapper_4_22.pdf.

of January 2017.[103] It is now March, and the administration has issued neither the estimate nor any public response to the members' second letter.

This basic information is necessary for Americans to evaluate the impact of Section 702 on their privacy. It is also necessary because most Americans are not lawyers, and when they hear that a surveillance program is "targeted" only at foreigners overseas and that any acquisition of Americans' communications is "incidental," they may reasonably assume that there is very little collection of their own calls and e-mails. An estimate of how many communications involving Americans are collected would help to pierce the legalese and give Americans a truer sense of what the program entails.

In short, Section 702 is a public statute that is subject to the democratic process, and the democratic process cannot work when Americans and lawmakers lack critical information. More transparency is urgently needed so that the country can begin an informed public debate about the future of foreign intelligence surveillance.

Thank you again for this opportunity to testify.

[103] *See* Press Release, U.S. House Comm. on the Judiciary Democrats, Bipartisan House Coalition Presses Clapper for Information on Phone & Email Surveillance (Dec. 16, 2016), *available at* https://democrats-judiciary.house.gov/news/press-releases/bipartisan-house-coalition-presses-clapper-information-phone-email-surveillance.

Mr. MARINO. Thank you.
Mr. Klein.

TESTIMONY OF ADAM KLEIN, SENIOR FELLOW, CENTER FOR A NEW AMERICAN STRATEGY

Mr. KLEIN. Thank you, Mr. Chairman and Members of the Committee. Thank you for inviting me to testify today.

My name is Adam Klein. I'm a senior fellow at the Center for a New American Security, which is a bipartisan research organization that develops strong, pragmatic national security and defense policies.

In a recent report, two colleagues and I offered more than 60 recommendations for the future of surveillance policy, including Section 702. Our research was informed by private consultations with dozens of current and former government officials, technology experts, legal scholars, and privacy advocates.

We concluded that Section 702 is a valuable intelligence tool and should be reauthorized with current authorities intact. In particular, we were moved by the measured but largely positive judgment of the bipartisan Privacy and Civil Liberties Oversight Board, which concluded that the program has been valuable and effective, found no evidence of intentional abuse, and reported that over a quarter of the NSA's reports on international terrorism were based in whole or in part on Section 702.

Our report also noted, however, that important intelligence programs, including Section 702, will not be politically sustainable unless the public has confidence that they're being used in a lawful and appropriate way and that they are subject to strong oversight. So the challenge for us is to enhance public trust without diminishing Section 702's effectiveness as an intelligence tool.

My written testimony lists more than a dozen concrete actionable ways Congress can do this as part of this process. I'll just highlight a few here.

First, and I think this is the most urgent issue facing the Committee during the reauthorization process, Congress needs to revive the Privacy and Civil Liberties Oversight Board. The Board has provided excellent oversight of Section 702. Its positive judgment about the program is one of the best arguments for why the program should be reauthorized. Unfortunately, the Board is now paralyzed because it has no chairman and has too few members to take official action.

My written testimony contains several proposals for reviving and enhancing the Board. I'll just note one here. The Foreign Intelligence Surveillance Court, before it issues the annual order that allows Section 702 to operate, should be required to confirm that the President has made nominations to any vacancies on the Board. This will give Presidents a real incentive to nominate members to the Board, something that has been a problem since the Board was created.

Another area where there's room for pragmatic reform is queries of Section 702 information using U.S. person identifiers, especially FBI queries in criminal investigations that are not related to national security. This practice does raise real civil liberties concerns.

But at the same time, there are reasons not to prohibit these queries altogether or at least to be very cautious before doing so.

The 9/11 Commission explained that the inability to connect the dots between domestic law enforcement and foreign intelligence was a key reason why the government did not disrupt the 9/11 attacks. If there's a connection between the subject of an FBI investigation in the United States and a foreign terrorist or a spy or a proliferator who has been targeted under 702, we want the FBI to know that.

Now, that said, there are ways to address privacy concerns short of banning these queries altogether. The most important is transparency. So the government should provide more information about the number of such queries, about how often they return Section 702 information, and about how the Justice Department uses that information downstream in the criminal justice system.

Another possibility worth exploring is whether the FBI could continue running all the queries it runs today but in some subset of them receiving only the metadata of the responsive communications initially instead of the underlying content. That could be enough to reveal any connections to problematic foreign actors.

One final recommendation I'd like to highlight. The USA FREEDOM Act created a pool of cleared advocates to present public interest arguments before the FISA court. Now, whether to appoint one of those advocates is currently in the court's discretion. We believe that Congress should make it mandatory in at least one case a year: the court's annual review of Section 702. That's a very easy way to strengthen judicial oversight of 702 with absolutely no costs for national security.

Thank you, and I look forward to your questions.

[The testimony of Mr. Klein follows:]

March 1, 2017

Testimony before the House Committee on the Judiciary

Hearing on Section 702 of the Foreign Intelligence Surveillance Act

Adam Klein
Senior Fellow, Center for a New American Security

—

Executive Summary

Findings

- Credible, unclassified assessments—most notably the landmark report of the independent Privacy and Civil Liberties Oversight Board—confirm that Section 702 is a valuable intelligence tool that is legitimate in its basic contours and subject to adequate oversight and transparency in most respects.
- Since the 2012 reauthorization, the USA Freedom Act and the recommendations of the Privacy and Civil Liberties Oversight Board have significantly strengthened the oversight, transparency, and privacy protections applicable to Section 702.
- Section 702 should be reauthorized with its current substantive authorities intact, but with reforms to further enhance transparency and strengthen oversight.
- The Privacy and Civil Liberties Oversight Board's uncertain future is an urgent problem and is inextricably connected to reauthorization of Section 702. Reauthorization should thus be accompanied by legislative measures to save and strengthen this important oversight body.
- An estimate of the scale of incidental collection of U.S.-person information under Section 702 would help inform public debate. Unfortunately, there remain practical obstacles to generating such an estimate.
- The FBI's U.S.-person queries of databases containing 702 data, particularly in non-national-security criminal investigations, raise civil liberties concerns. At the same time, there are colorable reasons for not prohibiting such queries altogether. Greater transparency is needed to better inform the public debate over this practice.
- The analogous capabilities of other countries—including member states of the European Union, which has criticized U.S. surveillance practices as inadequately privacy protective—are subject to less-rigorous legal constraints, oversight mechanisms, and transparency requirements than Section 702.

Recommendations

1. Reauthorize Section 702 with current authorities intact, but with the following reforms to enhance transparency and oversight:
2. Mandate that the Foreign Intelligence Surveillance Court appoint a cleared amicus curiae in every review of an annual certification under Section 702.
3. Require the Foreign Intelligence Surveillance Court to confirm, as a condition of approving the Attorney General and DNI's annual 702 certification, that the President has nominated candidates for any vacancies on the Privacy and Civil Liberties Oversight Board.
4. Exempt the Privacy and Civil Liberties Oversight Board from the Government in the Sunshine Act, which hampers the Board's efforts to oversee sensitive counterterrorism programs.
5. Empower the remaining members of the Privacy and Civil Liberties Oversight Board to collectively exercise the authorities of the Chairman when that position is vacant.
6. Ensure full implementation of Recommendation 9 from the Privacy and Civil Liberties Oversight Board's report on Section 702, including public disclosure (to the extent consistent with national security) of the resulting data about the collection and use of U.S.-person information under Section 702.
7. Encourage the intelligence community to continue to seek a statistically valid, feasible methodology for estimating the volume of incidental collection of U.S.-person data under Section 702. If these efforts do not succeed, consider creating a technical working group, perhaps under the auspices of the National Academy of Sciences, to attempt to formulate a viable approach.
8. Ask the FBI to publicly explain in greater detail why it needs to retain the ability to query databases containing Section 702 information for U.S.-person identifiers.
9. Ask the FBI to consider and explain whether it would be sufficient for it to continue its current practice of querying databases containing 702 data in non-national-security criminal investigations but, where such a query returns a hit, to initially view only the responsive metadata rather than the content.
10. Require the FBI to publish the aggregate number of annual instances in which "FBI personnel receive and review Section 702-acquired information that the FBI identifies as concerning a United States person in response to a query that is not designed to find and extract foreign intelligence information," a count already compelled by the Foreign Intelligence Surveillance Court.
11. Consider requiring the FBI to estimate the total number of instances in which FBI agents conducting non-national-security criminal investigations query databases containing Section 702 data using U.S.-person identifiers.
12. Require the Justice Department to provide greater detail about which "crimes involving … cybersecurity" would qualify as "serious crimes" for which the government would use 702-derived information in a criminal case.

13. Require the Justice Department to publish its standard for standard for determining whether evidence introduced in a criminal proceeding is "derived from" 702 information, which requires notice to the defendant.
14. Compare the legal, oversight, and policy constraints on Section 702 with those applicable to the analogous capabilities of other countries, particularly those countries that have used economic leverage to challenge U.S. surveillance practices.
15. Consider, as part of 702 reauthorization, using either legislative findings or report language to confirm for European audiences that the Judicial Redress Act remains in effect and, as a duly enacted statute, binds the Executive Branch.

I. INTRODUCTION

Chairman Goodlatte, Ranking Member Conyers, and members of the Committee, thank you for the opportunity to testify today. In today's chaotic world, our country faces a complex array of national security threats, both from adversary nations and from non-state terrorist groups. Recently retired Director of National Intelligence James Clapper said last year that in his 50-year career in intelligence, he could not "recall a more diverse array of challenges and crises than we confront today."[1]

In this challenging geopolitical context, the American people are fortunate to have the world's most capable intelligence services. Intelligence Community personnel work to protect the American people from a range of threats—from terrorism, to the theft of American companies' trade secrets, to subversion of our democratic processes by foreign intelligence services. In a digital world, signals intelligence is an essential tool for detecting and defeating these threats.

Our intelligence agencies, led by the NSA, carry out the signals intelligence mission under what the President Obama's Review Group on Intelligence and Communications Technologies described as a system of "oversight, review, and checks-and-balances" that "reduce[s] the risk that elements of the Intelligence Community would operate outside of the law."[2] The Review Group, which President Obama commissioned in the wake of the Snowden leaks to review U.S. signals intelligence activities, emphasized in its report that it had found "no evidence of illegality or other abuse of authority for the purpose of targeting domestic political activity."[3] That accords with other reports that have emphasized the deep-rooted culture of compliance and legal oversight at NSA.[4]

At the same time, the Snowden leaks revealed that the scale of government data collection—even collection that was lawful and approved by the Foreign Intelligence Surveillance Court—was greater than most Americans would have anticipated given the available public information, including the text of the relevant statutes. The resulting climate of skepticism, at home and abroad, continues to harm U.S. interests in various ways.[5]

This is not simply a privacy or civil liberties problem: If allowed to persist, public skepticism is also a problem for national security. That is because public trust is the foundation on which national security powers, including Section 702, ultimately rest. Needed surveillance tools will be politically sustainable only if the public is persuaded that they are necessary, appropriate, and lawful. For that reason, strengthening public confidence in the legal and institutional controls on surveillance powers should be seen as a national security imperative as well as a priority for civil libertarians.

The challenge is how to strengthen transparency, privacy, oversight, and ultimately public confidence without harming needed national security capabilities. In a recent Center for a New American Security report, *Surveillance Policy: A Pragmatic Agenda for 2017 and Beyond*, coauthors Michèle Flournoy, Richard Fontaine, and I offered 61 recommendations to build public trust, increase transparency, and strengthen oversight, while preserving important intelligence and counterterrorism tools. Part III of this testimony suggests a number of ways the Committee can advance these goals while reauthorizing Section 702.

II. SECTION 702'S VALUE FOR NATIONAL SECURITY

In our recent report, my co-authors and I concluded, based on the available unclassified sources, that Section 702 "has become a vital intelligence tool, is legitimate in its basic contours, and is subject to adequate transparency in many, but not all, respects."[6] For that reason, we recommended that Section 702 be reauthorized with current authorities intact, but with reforms to enhance transparency and oversight.

The Committee has access to classified information documenting Section 702's value for foreign intelligence and counterterrorism, but most Americans do not. This section briefly summarizes for the general public the unclassified assessments that my co-authors and I found persuasive in reaching our judgment.

The most significant unclassified review of Section 702's efficacy and legality remains the landmark report by the independent Privacy and Civil Liberties Oversight Board.[7] The Board's five members, three Democrats and two Republicans, received classified briefings from the Intelligence Community and Department of Justice, but also consulted with outside civil-society groups, academics, and technology companies. The Board documented its findings and conclusions in a 160-page report, which provided an important public service by explaining for the American public many previously classified details about how 702 operates: the program's PRISM and upstream components, the court-approved targeting and minimization procedures that constrain the agencies' use of these tools and the data they generate, and the multi-layered oversight system that ensures compliance with these rules.

After this review, the Board unanimously reached a measured but broadly positive conclusion about the overall utility, lawfulness, and oversight of Section 702:

> "[T]he information the program collects has been valuable and effective in protecting the nation's security and producing useful foreign intelligence. The program has operated under a statute that was publicly debated, and the text of the statute outlines the basic structure of the program. Operation of the Section 702 program has been subject to judicial oversight and extensive internal supervision, and the Board has found no evidence of intentional abuse."[8]

Publicly available statistics declassified by the Office of the Director of National Intelligence suggest that Section 702 has become a central foreign intelligence tool. Overall, in 2015, the intelligence community targeted 94,368 overseas individuals, groups, or entities under Section 702.[9] That is compared to only 1,695 targets of orders issued under "traditional" FISA.[10] While this is not an apples-to-apples comparison, it does give a rough sense of the significance of Section 702 for our foreign intelligence enterprise.

The available evidence also indicates that Section 702 has been a particularly significant tool for counterterrorism. The Privacy and Civil Liberties Oversight Board reported that, as of 2014, "over a quarter of the NSA's reports concerning international terrorism include information based in whole or in part on Section 702 collection, and this percentage has increased every year since the statute was enacted."[11] The Board also found that "[m]onitoring terrorist networks under Section

702 has enabled the government to learn how they operate, and to understand their priorities, strategies, and tactics"; that it "has led the government to identify previously unknown individuals who are involved in international terrorism"; and that it "has played a key role in discovering and disrupting specific terrorist plots aimed at the United States and other countries."[12]

Other sources echo the Board's judgment that Section 702 is a vital tool for counterterrorism and foreign intelligence more broadly. Matthew Olsen, former General Counsel of NSA and former Director of the National Counterterrorism Center, told this Committee's Senate counterpart last spring that Section 702 "has proven to be a vital authority for the collection of foreign intelligence to guard against terrorism and other threats to our national security" and "has significantly contributed to our ability to prevent terrorist attacks inside the United States and around the world."[13] NSA has publicly described Section 702 as the "most significant tool in the NSA collection arsenal for the detection, identification, and disruption of terrorist threats to the U.S. and around the world."[14]

III. Civil Liberties Safeguards and Concerns

As the Privacy and Civil Liberties Oversight Board explained, Section 702 is subject to both "judicial oversight and extensive internal supervision."[15] To be sure, judicial oversight of Section 702 differs significantly from judicial review under traditional FISA: The Foreign Intelligence Surveillance Court reviews the Section 702 program *as a whole*, on an annual basis, rather than reviewing each target individually. Once a year, the Director of National Intelligence and the Attorney General must submit to the FISC a joint "certification" specifying how the program will be administered and what safeguards apply.[16] The FISC then reviews and approves or disapproves that certification, as well as agency minimization and targeting procedures, subject to any conditions the court imposes.[17] As required by the USA Freedom Act, many significant FISC opinions, including the court's review of the 2015 Section 702 certification, have been declassified and published.[18]

As we wrote in our recent Center for a New American Security report, programmatic rather than individualized judicial review is appropriate for Section 702 "given that the targets are non-U.S. persons living outside the United States."[19] Section 702 occupies, legally speaking, a novel middle ground between traditional domestic surveillance under FISA and overseas surveillance governed by Executive Order 12333. Traditional FISA requires, generally speaking, individualized judicial orders for foreign-intelligence surveillance, conducted in the United States, of those *present in the United States*.[20] By contrast, those targeted under Section 702—non-U.S. persons overseas—are not protected by the Fourth Amendment,[21] and their messages to other non-Americans have traditionally been subject to surveillance without judicial oversight.[22] On the other hand, 702 surveillance transpires on U.S. soil and foreseeably results in the interception of a significant (but unknown) number of messages with one U.S. communicant, which previously could have been collected on U.S. soil only with a FISA warrant.[23] Section 702's annual, programmatic judicial oversight strikes a reasonable middle ground between the geographic location of the surveillance (in the U.S.), the geographic location and nationality of the targets (non-U.S. persons located overseas), and the foreseeable consequence that some messages with a U.S. communicant will be collected.

Surveillance under Section 702, and the subsequent retention and dissemination of information it produces, must also comply with detailed, 702-specific targeting and minimization

procedures, which are reviewed and approved by the Foreign Intelligence Surveillance Court during its annual review.[24] The Office of the Director of National Intelligence has published online, with relatively few redactions, the 702 minimization rules for the NSA, FBI, CIA, and National Counterterrorism Center.[25] Recent compliance assessments by the Attorney General and the Office of the Director of National Intelligence have found a low rate of inadvertent "compliance incidents" and no intentional attempts to circumvent these rules.[26]

It is important to note that the implementation and oversight constraints applicable to Section 702 have changed significantly since the program's last reauthorization five years ago. Since the Snowden leaks in 2013, Section 702 has undergone many significant privacy, transparency, and governance reforms. Most importantly, the government has fully implemented most of the recommendations in the Privacy and Civil Liberties Oversight Board's report on Section 702, and is working to implement those that remain. These include:

- Revising the FBI's minimization procedures to accurately reflect its querying of 702 data in investigations unrelated to foreign intelligence,[27]
- Requiring better documentation of the foreign-intelligence purpose of NSA and CIA queries of 702 data using U.S.-person identifiers,[28]
- Enhancing the FISC's ability to review 702 targeting practices and U.S.-person query terms used by the NSA and CIA,[29]
- Periodically reassessing whether upstream collection under Section 702 uses the best available technology to ensure that only authorized communications are collected,[30] and
- Making publicly available the current NSA, CIA, and FBI minimization procedures for Section 702.[31]

In addition, the USA Freedom Act implemented a number of changes with spillover benefits for accountability and oversight of Section 702. These include:

- Enabling the Foreign Intelligence Surveillance Court to appoint cleared amici curiae to present "legal arguments that advance the protection of individual privacy and civil liberties" in cases presenting novel legal issues,[32]
- Expanding appellate review of FISC decisions,[33]
- Releasing to the public, to the extent consistent with national security, past and future FISC decisions in cases presenting significant or novel issues,[34] and
- Allowing private companies subject to FISA orders to provide the public with more detail about the volume of surveillance orders they receive.[35]

One relatively simple way for Congress to build on this progress and further strengthen 702 oversight would be to mandate the appointment of a FISC amicus curiae in every review of annual certifications under Section 702. One of the cleared FISC advocates, Amy Jeffress, participated constructively in the FISC's review of the government's 2015 certifications for the Section 702 program.[36] Under current law, whether to appoint an amicus is in the court's discretion.[37]

Guaranteeing that an amicus will be appointed in this narrow, but very important, category of cases would strengthen the public credibility of Section 702's programmatic judicial oversight.

The Privacy and Civil Liberties Oversight Board

In my opinion, the most urgent privacy and civil liberties issue before the Committee during this reauthorization process is the crisis facing the Privacy and Civil Liberties Oversight Board. This is somewhat counterintuitive, as the Board was not created by the FISA Amendments Act and its responsibilities are broader than Section 702. In recent years, however, the Board has been an essential source of public-facing oversight and accountability for the government's implementation of Section 702. Unfortunately, the Board is now in crisis, unable to take official action and in danger of fading into permanent paralysis.

The Board emerged from a recommendation of the 9/11 Commission, which called for a "board within the executive branch to oversee … the commitment the government makes to defend our civil liberties."[38] Since 2013, the Board has become a prominent feature of the oversight landscape for counterterrorism and surveillance programs. Most important have been the Board's comprehensive and well-regarded public reports—particularly its report on Section 702, which enhanced public understanding by declassifying many basic facts about how the program operates.

Importantly, the Board's value extends beyond privacy and civil liberties: A credible, independent Board also benefits national security and the intelligence community. Precisely because of the Board's independence and bipartisan credibility, its statement that Section 702 is "valuable and effective" provides a powerful argument for reauthorizing the program in its current form. The Board's reputation as a vigorous and independent voice also helps intelligence officials make the case to other countries that U.S. surveillance programs are subject to robust oversight and legal controls. For example, in a letter designed to address European concerns related to the Privacy Shield agreement, the General Counsel of the Office of the Director of National Intelligence cited the Board and its public reports as evidence of the "rigorous and multi-layered" oversight of U.S. intelligence.[39]

Unfortunately, the Board is on the verge of becoming defunct: With only two of five Senate-confirmed members remaining, it lacks a quorum and thus cannot take official action. (One of those two remaining members has now been nominated for a senior position in the Justice Department.) Another institutional challenge is that without a Chairman, the Board has been unable to hire new staff since last summer.

The crisis facing the Board is intimately connected to reauthorization of Section 702. Strong national security powers—which we need to keep our country safe—must be balanced by strong and credible oversight. That comes first and foremost from the Congress, but also (subject to constitutional and statutory limits) from the courts and from internal Executive Branch bodies like the Board. As the Board's 702 report and its subsequent recommendations-assessment reports demonstrate, a functioning, independent Board is a key element of the "rigorous and multi-layered" oversight of Section 702.[40]

In reauthorizing Section 702, Congress should also act to revive the Board and ensure its future viability. Specifically, in the reauthorization legislation, Congress should require the FISC to confirm, as a condition of approving the Attorney General and DNI's annual 702 certification, that the President has nominated candidates for any vacancies on the Board.[41] This will ensure that Presidents have an adequate incentive to make nominations to the board. There is no reason why requiring nominations (as opposed to confirmation of those nominees) to be in place would obstruct or delay annual recertifications of the program.

In addition, to enhance the Board's functioning Congress should, as part of Section 702 reauthorization, enact legislation exempting the Board from the Government in the Sunshine Act. That statute requires that meetings—which are vaguely defined as "deliberations" involving more than two members—take place in public if they "result in the joint conduct or disposition of official agency business."[42] There are several reasons why this is unnecessary for the Board.

First, and most importantly, the Sunshine Act's purpose—ensuring that regulatory power is exercised in public rather than in smoke-filled back rooms—does not apply to the Board. The Board exercises no regulatory power; its only authorities are to conduct oversight and provide advice. For an oversight body, the benefits of informal collaboration far outweigh any possible concern about opaque decisionmaking. Indeed, because the Sunshine Act obstructs the Board's oversight work, it perversely *impedes* efforts to bring "sunshine" to counterterrorism programs.

Another reason why the Sunshine Act is a poor fit is that the Board's work is overwhelmingly classified. This means that it is forced to squander substantial time repeatedly invoking the Act's cumbersome procedures for closing meetings.[43] In addition, because four of the Board's five members are part-time and have outside obligations, their schedules make it challenging to hold frequent formal meetings. Congress should remove this nuisance, which, ironically undermines transparency by preventing the Board from being as effective as it might be.

Finally, to ensure that the Board is not hampered in the future by the absence of a Chairman, Congress should enact legislation permitting the remaining members to collectively exercise the authorities of the Chairman if the position of Chairman is vacant.[44]

Incidental Collection

Even with the many legal, oversight, and compliance safeguards in place, Section 702 raises legitimate concerns for domestic civil liberties. The most noteworthy is the incidental collection of communications of or about U.S. persons and the subsequent use of such information. While Section 702 cannot be used to *target* U.S. persons, their communications can be "incidentally collected" if they communicated with a targeted non-U.S. person. Foreign-foreign communications may also contain information about a U.S. person, even if he or she is not one of the communicants.

No one knows how much U.S.-person information is incidentally collected under Section 702. As the Privacy and Civil Liberties Oversight Board explained: "[L]awmakers and the public do not have even a rough estimate of how many communications of U.S. persons are acquired under Section 702."[45] The public debate over Section 702's implications for domestic civil liberties would

be better informed if the public had a more accurate sense of how much U.S.-person data is collected.

Recommendation 9 in the Privacy and Civil Liberties Oversight Board's report on Section 702 urged the NSA to track five measures that would "shed some light on the extent to which communications involving U.S. persons or people located in the United States are being acquired and utilized under Section 702."[46] These were:

1. The number of telephone communications acquired in which one caller is located in the United States;
2. The number of Internet communications acquired through upstream collection that originate or terminate in the United States;
3. The number of communications of or concerning U.S. persons that the NSA positively identifies as such in the routine course of its work;
4. The number of queries performed that employ U.S. person identifiers, specifically distinguishing the number of such queries that include names, titles, or other identifiers potentially associated with individuals; and
5. The number of instances in which the NSA disseminates non-public information about U.S. persons.[47]

As of last February, NSA had implemented two of these measures in substantial part, but had "confronted a variety of challenges" in implementing the final three.[48] As it works toward reauthorizing Section 702, Congress should ensure that NSA fully implements Recommendation 9, and should encourage the maximum public reporting of these figures that is consistent with national security.

Some members of this Committee and a number of advocacy groups have urged NSA to attempt a statistical estimate of all incidental collection, by counting the number of U.S.-person communications within a representative sample of communications gathered under 702.[49] The government has noted that such a review would inflict some additional privacy harm on those Americans whose incidentally collected communications would otherwise have "aged off" NSA servers before being reviewed.[50] On balance, however, this limited harm would be justified by the benefits an estimate of incidental collection would produce for public accountability—*if* a statistically valid, feasible methodology of conducting such an estimate can be found.

Unfortunately, a viable methodology has proven difficult to find, and ultimately may not exist. The primary reason is that electronic communications collected under Section 702 typically lack information that would enable officials to determine the nationality of the communicants. Emails, for example, do not list the nationality of the sender and recipient, much less of people mentioned in the body text. Undertaking additional investigation beyond the four corners of the communication to determine the nationality of the communicants and others discussed in the message would be intrusive from a privacy perspective and unreasonably labor-intensive.

Given the potential value of a valid estimate, it is worth continuing to attempt to surmount these obstacles, even if no practicable solution is ultimately found. Our report thus recommended that the intelligence community persist in seeking to develop an approach that would yield an accurate, statistically valid estimate of incidental collection. If these efforts do not succeed, Congress should consider convening a technical working group, perhaps under the auspices of the National Academy of Sciences, to attempt to develop a viable approach.[51]

U.S.-Person Queries

One of the most challenging civil-liberties issues facing Congress during the reauthorization process is the practice of querying Section 702 data for U.S.-person identifiers—particularly in criminal investigations unrelated to national security. As a routine investigative step, FBI agents and analysts may check to see what information the Bureau's records already contain about a person. At least one of those databases contains foreign intelligence information, including intelligence collected both under Section 702 and from traditional FISA.[52] While the Foreign Intelligence Surveillance Court has held that such queries comport with the Fourth Amendment,[53] they nonetheless raise legitimate privacy concerns—particularly if such information flows downstream into the criminal justice system.

On the other hand, there are also colorable arguments for not prohibiting such queries altogether. The 9/11 Commission explained that one of the key reasons the 9/11 attacks succeeded was the government's failure to synthesize pieces of information that different agencies possessed. Put simply, government agencies failed to "connect the dots" in time to disrupt the attacks.[54] This failure was particularly pronounced across what the Commission termed the "foreign-domestic divide"—the gap between foreign intelligence and domestic law-enforcement investigations. For example, within the Justice Department and FBI, many believed that the Bureau "could not share any intelligence information with criminal investigators," with the result that "relevant information from the National Security Agency and the CIA often failed to make its way to criminal investigators."[55] These information-sharing blockages contributed to the tragic failure to locate 9/11 hijacker Khalid al Mihdhar, whom the government knew had entered the United States.[56] Had Mihdhar been arrested, the government might well have foiled the 9/11 attacks.[57]

If there is a connection between a person under FBI investigation in the United States and foreign-intelligence information the government has already collected under 702—including the communications of known terrorists—it is important for the FBI to be aware of that. Indeed, Section 702 is particularly likely to identify connections relevant to transnational threats like terrorism, foreign espionage, and proliferation. That is because Section 702 is used to target individuals of foreign-intelligence interest (that is, non-U.S. "persons assessed to possess foreign intelligence information or who are reasonably likely to receive or communicate foreign intelligence information").[58] If an FBI agent conducting a domestic investigation receives a hit when querying 702 information, that means that the subject of the query communicated with, or was mentioned in a communication to or from, a person of foreign-intelligence interest. Some (perhaps many) such connections will be innocent, but others will be problematic and previously unknown to investigators. The latter represent the type of foreign-domestic linkages that can help the FBI detect and prevent terrorist attacks.

Unfortunately, relatively little public information is available about these queries: their frequency, how often they return 702 information, and precisely why the FBI views them as valuable. The result is that estimates of both the practice's value for national security and its civil-liberties implications are unavoidably conjectural. Greater transparency is needed to better inform the public debate. Our recent report offered several recommendations in this vein.

First, the FBI should publicly explain in greater detail why it values the ability to query databases containing Section 702 information for U.S.-person identifiers. In so doing, it should also explain why other investigative techniques would not be as effective. To be sure, there may be persuasive answers to these questions.[59] Even so, more information about the role these queries play in FBI investigations and the suitability of possible alternatives could help strengthen the public legitimacy of this practice.

Second, Congress should ask the Bureau to consider whether an alternative form of these queries would suffice to enable it to identify previously unknown, problematic foreign-domestic connections. Specifically, the FBI should consider and explain whether it would be sufficient for it to continue its current practice of querying databases containing 702 data in non-national-security investigations but, where such a search returns a hit, *to view only the responsive metadata* rather than the content.

This is worth considering because the key function of these queries appears to be identifying previously unknown, potentially significant foreign-domestic links. In most cases, the metadata of responsive communications should suffice to reveal those connections. If metadata suggests a problematic connection, it could be used to establish individualized suspicion to view the underlying content and to deploy other investigative tools in the FBI's arsenal.

Third, as part of Section 702's reauthorization, Congress should provide for increased public transparency about the querying and use of 702 information about U.S.-persons in non-national-security FBI investigations. The FBI reports that it is "extremely unlikely that an agent or analyst who is conducting an assessment of a non-national-security crime would get a responsive result from the query against the [FBI's] Section 702-acquired data."[60] One possible reason for this is that the FBI does not receive data from 702's upstream component, which for technical reasons "has a higher likelihood than PRISM of collecting … some wholly domestic communications."[61]

If there is indeed a reassuring story to tell here, greater public transparency would help the FBI tell it. To that end, Congress should:

i. Require the FBI to publish the number of annual instances in which "FBI personnel receive and review Section 702-acquired information that the FBI identifies as concerning a United States person in response to a query that is not designed to find and extract foreign intelligence information."[62] The FISC already requires the Bureau to report these instances to the Court,[63] so counting them should not impose an additional administrative burden. While the details of these reports must remain classified, it is hard to imagine any national security harm that would result from publishing the overall number of such occurrences.

ii. Consider requiring the FBI to estimate the total number of instances in which FBI agents conducting non-national-security criminal investigations query databases containing Section 702 data using U.S.-person identifiers. The FBI's systems are not designed to "identify whether the query terms are U.S.-person identifiers,"[64] because "nationality is not relevant to most criminal investigations."[65] The Bureau should not be asked to revamp its record-keeping system in order to produce this data; a statistically representative sample of cases would suffice.

Fifth, Congress should require increased public transparency about the downstream use in the criminal-justice system of information derived from Section 702. Specifically:

i. Congress should require the Justice Department to provide greater detail about which "crimes involving … cybersecurity"—a broad category potentially encompassing both very grave and less consequential offenses[66]—would qualify as "serious crimes" for which the government would use 702-derived information in a criminal case.[67]

ii. Congress should also require the Justice Department to publish its standard for whether evidence introduced in a criminal proceeding was "derived from" 702 information, which requires notice to the defendant.

IV. Section 702 in International Perspective

Since 2013's Snowden leaks, the United States has faced international pressure over its surveillance practices, particularly from the European Union. This pressure has been heightened by the leverage that European privacy law provides over U.S. companies' transfers of European data to the United States. The scramble in late 2015 and early 2016 to find a replacement to the U.S.-EU Safe Harbor agreement, and the concessions that the United States made to obtain the successor Privacy Shield accord, demonstrate that this leverage is significant.[68]

It is in the U.S. national interest to reduce conflict with Europe over surveillance policy—in particular, to ensure that the economically important Privacy Shield agreement remains in force. That does not mean, however, that the United States should make additional unreciprocated concessions to European critics of U.S. surveillance practices. More to the point: Congress should not materially alter Section 702 in an attempt to appease European critics. To begin with, the significant unreciprocated concessions that the United States already made in the wake of the Snowden leaks are not well known in Europe and have generated little goodwill for the United States. For example, one German expert told our CNAS team that most Germans are "totally unaware" of Presidential Policy Directive 28, a commitment without apparent historical precedent, and which no other country has matched. What's more, European allies benefit directly from Section 702 by way of intelligence sharing from the United States. The problem is that European security services have little incentive, and ample political disincentive, to publicize this cooperation.

A better approach to shoring up Privacy Shield would be for the United States to demonstrate that the terms of that agreement are being robustly enforced, while at the same time (i) encouraging an amicable comparison between our legal and oversight regime and those of our European allies, and (ii) quietly demonstrating to Europe that the United States has a "Plan B,"

other than further unilateral concessions, should the European Court of Justice issue another flawed decision like *Schrems v. Data Protection Commissioner*. That decision, which effectively killed the Safe Harbor agreement, was informed, at least in part, by an inaccurate understanding of Section 702. Our recent Center for a New American Security report proposes numerous concrete steps the United States can take to effectuate this approach.[69]

In particular, the United States should welcome and encourage a comparison between its privacy and oversight regime and Europe's. Since the Snowden leaks, the U.S. has made commitments to respect the privacy rights of Europeans that far outstrip anything European nations have done in return. For example, no European country has reciprocated for Americans the commitments in Presidential Policy Directive 28. The closest comparator of which I am aware is Germany's recent law, analogous to Section 702, governing domestic collection of foreign-foreign communications.[70] That law grants heightened privacy protections to EU institutions, EU member states, and EU citizens, but nothing for Americans. Nor have EU member states offered Americans a privacy Ombudsperson and judicial-redress rights like those the United States gave Europeans as part of the Privacy Shield.[71]

More broadly, the United States' legal and oversight regime for government surveillance, including against non-U.S. persons, is equivalent to or stronger than the systems in place in leading European countries. Only two of the EU countries analyzed in a study by the law firm Sidley Austin "require judicial authorization for intelligence surveillance"; instead, "most place such authorization in the hands of government ministers."[72] Most relevant here, France, Germany, the United Kingdom, and the Netherlands all "explicitly permit certain types of surveillance that," unlike the selector-based Section 702, "are not targeted at identified suspected individuals."[73] None of these countries' laws explicitly require minimization, while retention limits apply only to a few narrow categories of data.[74]

This reauthorization process offers an opportunity to correct misperceptions about Section 702 that are widely held overseas. To that end, Congress can perform a valuable public service by comparing, whether through hearings or oversight reports, the substantive scope of Section 702 and the applicable legal constraints, oversight mechanisms, and transparency requirements, with the analogous programs of other countries—particularly countries that have criticized the United States for its surveillance practices.

One final issue bears brief mention here. The recent Executive Order on "Enhancing Public Safety in the Interior of the United States" ordered federal agencies, "to the extent consistent with applicable law," to "ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information."[75] This triggered alarm among some privacy advocates, and apparently some European observers, that the order had revoked protections that the United States promised European citizens as part of the Privacy Shield. That was incorrect: The Judicial Redress Act of 2015 extends the relevant rights by statute, which could not be (and thus was not) superseded by the Executive Order.[76]

Clearing up any such misconceptions and clarifying that the elements of the deal underlying Privacy Shield remain in place could increase the odds that it survives European judicial review. To

that end, Congress should consider, as part of 702 reauthorization, using either legislative findings or report language to confirm that the Judicial Redress Act remains in effect and, as a duly enacted statute, binds the Executive Branch.

Thank you again for the opportunity to testify.

***

ENDNOTES

[1] Mark Landler, *North Korea Nuclear Threat Cited by James Clapper, Intelligence Chief*, N.Y. Times, Feb. 9, 2016, *available at* http://www.nytimes.com/2016/02/10/world/asia/north-koreanuclear-effort-seen-as-a-top-threat-to-the-us.html.

[2] President's Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World* 75 (Dec. 12, 2013).

[3] *Id.* At 31-32.

[4] *See, e.g.*, Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* 103 (July 2, 2014), *available at* https://www.pclob.gov/library/702-Report.pdf ("The Board has been impressed with the rigor of the government's efforts to ensure that it acquires only those communications it is authorized to collect, and that it targets only those persons it is authorized to target. Moreover, the government has taken seriously its obligations to establish and adhere to a detailed set of rules regarding how it handles U.S. person communications that it acquires under the program.") (hereinafter "PCLOB 702 Report").

[5] *See* A. Klein, M. Flournoy, & R. Fontaine, *Surveillance Policy: A Pragmatic Agenda for 2017 and Beyond* 17-21 (Dec. 2016), *available at* https://s3.amazonaws.com/files.cnas.org/documents/CNAS-Report-Surveillance-Final.pdf (hereinafter "CNAS Surveillance Policy Report").

[6] CNAS Surveillance Policy Report, *supra* note 5, at 24.

[7] PCLOB 702 Report, *supra* note 4.

[8] *Id.* at 2.

[9] Office of the Director of National Intelligence, *Statistical Transparency Report Regarding Use of National Security Authorities for Calendar Year 2015*, at 5, *at* https://www.dni.gov/files/icotr/ODNI%20CY15%20Statistical%20Transparency%20Report.pdf.

[10] *Id.* at 4.

[11] *Id.* at 10.

[12] *Id.*

[13] Testimony before the Senate Committee on the Judiciary (May 10, 2016), *at* https://www.judiciary.senate.gov/imo/media/doc/05-10-16%20Olsen%20Testimony.pdf.

[14] NSA, *The National Security Agency: Missions, Authorities, Oversight and Partnerships* (Aug. 9, 2013), *at* https://www.nsa.gov/news-features/press-room/statements/2013-08-09-thensa-story.shtml.

[15] PCLOB 702 Report, *supra* note 4, at 2.

[16] *See* 50 U.S.C. § 1881a(g).

[17] *See* 50 U.S.C. § 1881a(i).

[18] *See infra* note 24.

[19] CNAS Surveillance Policy Report, *supra* note 5, at 24.

[20] *See* 50 U.S.C. § 1801 *et seq.* Other provisions of the FISA Amendments Act require individualized judicial orders to target *U.S. persons* overseas. *See* 50 U.S.C. §§ 1881b-1881c.

[21] *See United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990). *Verdugo* includes the caveat that the alien involved lacked a preexisting "substantial connection" to the United States. *Id.* at 271-272.

[22] *Cf.* Chris Inglis & Jeff Kosseff, *In Defense of FAA Section 702*, Hoover Institution Aegis Paper Series, No. 1604 (2016), *at* http://www.hoover.org/sites/default/files/research/docs/ingliskosseff_defenseof702_final_v3_digital.pdf.

[23] *See* 50 U.S.C. § 1801(f)(2); David Kris, *Trends and Predictions in Foreign Intelligence Surveillance: The FAA and Beyond*, Hoover Institution Aegis Paper Series No. 1601, at 3 (2016), *at* http://www.hoover.org/sites/default/files/research/docs/kris_trendspredictions_final_v4_digital.pdf.

[24] *See, e.g.*, Memorandum Opinion and Order, No. [redacted], at 12 (F.I.S.C. Nov. 6, 2015), *at* https://www.dni.gov/files/documents/20151106-702Mem_Opinion_Order_for_Public_Release.pdf (hereinafter "2015 FISC Opinion").

[25] Office of the Director of National Intelligence, *Release of 2015 Section 702 Minimization Procedures* (Aug. 11, 2016), https://icontherecord.tumblr.com/tagged/section-702.

[26] *See* Department of Justice & Office of the Director of National Intelligence, *Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence* 27-28 (Nov. 2016).

[27] Privacy and Civil Liberties Oversight Board, Recommendations Assessment Report 16 (Feb. 5, 2016).

[28] *Id.* at 18.

[29] *Id.* at 19.

[30] *Id.* at 21.

[31] *Id.* at 23.

[32] *See* 50 U.S.C. § 1803(i).

[33] *See* PCLOB Recommendations Assessment Report, *supra* note 27, at 5-6.

[34] *See id.* at 7-8.

[35] *See id.* at 10.

[36] *See generally* 2015 FISC Opinion, *supra* note 24.

[37] *See* 50 U.S.C. § 1803(i).

[38] *See, e.g.*, National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* 395 (2004).

[39] Letter from Robert Litt to Justin Antonipillai, Counselor, Department of Commerce, and Ted Dean, Deputy Assistant Secretary, International Trade Administration (February 22, 2016), at 7, *at* http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-6_en.pdf.

[40] *See id.*

[41] *See* 42 U.S.C. § 2000ee(h)(1).

[42] 5 U.S.C. § 552b.

[43] *See* Patricia Wald, Responses to Sen. Chuck Grassley Questions for the Record 5, *at* https://www.judiciary.senate.gov/imo/media/doc/Wald-Reappoint-Responses-to-Grassley.pdf.

[44] *Cf.* S. 3017, Intelligence Authorization Act for Fiscal Year 2017, 114th Cong., § 602.

[45] PCLOB 702 Report, *supra* note 4, at 147.

[46] *Id.* at 146-147.

[47] *Id.* at 146.

[48] PCLOB Recommendations Assessment Report, *supra* note 27, at 25.

[49] Letter from House Judiciary Committee Members to Director of National Intelligence James Clapper (Apr. 22, 2016), *at* https://assets.documentcloud.org/documents/2811050/Letter-to-Director-Clapper-4-22.pdf; Letter from Privacy Groups to Clapper (Oct. 29, 2015), *at*

https://www.brennancenter.org/sites/default/files/analysis/Coalition_Letter_DNI_Clapper_102915.pdf.

[50] *See* PCLOB 702 Report, *supra* note 4, at 147.

[51] *Cf.* National Academies, *Committee Membership: Law Enforcement and Intelligence Access to Plaintext Information in an Era of Widespread Strong Encryption: Options and Tradeoffs* (Sept. 7, 2016), *at* https://www8.nationalacademies.org/cp/CommitteeView.aspx?key=49806.

[52] PCLOB 702 Report, *supra* note 4, at 59.

[53] 2015 FISC Opinion, *supra* note 24.

[54] *9/11 Commission Report* at 355-356.

[55] *Id.* at 79.

[56] *Id.* at 269-272.

[57] *See id.* at 272 (concluding that detention of Mihdhar or Nawaf al Hazmi "could have derailed the plan").

[58] PCLOB 702 Report, *supra* note 4, at 22 n.56.

[59] *See* CNAS Surveillance Policy Report, *supra* note 5, at 36.

[60] PCLOB 702 Report, *supra* note 4, at 60.

[61] Testimony of Rachel Brand before the Senate Committee on the Judiciary 5 (May 10, 2016), *at* https://pclob.gov/library/20160510-R%20Brand%20testimony%20SJC.pdf.

[62] *See* 2015 FISC Opinion, *supra* note 24, at 78.

[63] *See id.*; *see also DOJ/ODNI Semiannual Assessment*, *supra* note 26, at 16.

[64] PCLOB 702 Report, *supra* note 4, at 59.

[65] Brand Testimony, *supra* note 61, at 9.

[66] *See, e.g.*, *United States v. Nosal*, Nos. 14-10037 & 14-10275 (9th Cir. Dec. 8, 2016).

[67] *See* Remarks of Robert Litt at the Brookings Institution (Feb. 4, 2015), *at* https://icontherecord.tumblr.com/post/110099240063/video-odni-general-counsel-robert-litt-speaks-on; CNAS Surveillance Policy Report, *supra* note 5, at 38.

[68] *See id.* at 57.

[69] *See id.* at 50-57.

[70] *Available at* http://dip21.bundestag.de/dip21/btd/18/090/1809041.pdf; *see also* Library of Congress Global Legal Monitor, *Germany: Powers of Federal Intelligence Service Expanded*, *at* http://www.loc.gov/law/foreign-news/article/germany-powers-of-federal-intelligence-service-expanded/.

[71] *See* CNAS Surveillance Policy Report, *supra* note 5, at 53.

[72] Jacques Bourgeois et al., Sidley Austin LLP, *Essentially Equivalent: A comparison of the legal orders for privacy and data protection in the European Union and United States* 5 (Jan. 2016), http://www.sidley.com/~/media/publications/essentially-equivalent---final.pdf.

[73] *Id.* at 37.

[74] *Id.* at 51.

[75] *Available at* https://www.whitehouse.gov/the-press-office/2017/01/25/presidential-executive-order-enhancing-public-safety-interior-united.

[76] This is discussed in greater detail in *The "Interior Security" Executive Order, the Privacy Act, and Privacy Shield*, Carrie Cordero & Adam Klein, Lawfare, Jan. 27, 2017, *at* https://lawfareblog.com/interior-security-executive-order-privacy-act-and-privacy-shield.

Mr. MARINO. Thank you. We're now going to proceed into the 5-minute questioning, the three of us, and if anyone else shows up will have an opportunity to question you. I'm going to recognize myself for the first 5 minutes of questioning.

And, Mr. Kosseff, am I pronouncing that right, Kosseff?

Mr. KOSSEFF. Yes.

Mr. MARINO. And then I would like, if you care to, each member to answer my first question, which would be very simple. Is there anyone here that believes that we should not reauthorize this legislation?

Mr. KOSSEFF. I believe you should reauthorize.

Mr. MARINO. We should reauthorize?

Mr. KOSSEFF. Yes.

Ms. DOSS. I'm in favor of a clean reauthorization.

Ms. GOITEIN. I would be in favor of reauthorization if there were significant reform.

Mr. MARINO. Okay.

Mr. KLEIN. Yes, I support it as well, reauthorization.

Mr. MARINO. Ms. Goitein, you stated that, although not intentional at this point, did you say thousands or millions of names were gathered up, information was gathered up? Did I paraphrase that correctly? Did you say that you thought that there were thousands or there may be even millions of names or information gathered up unintentionally?

Ms. GOITEIN. Not unintentionally. It's part of the incidental collection. The terminology gets mixed up. "Incidentally" is the terminology that's used by the government. But it is part of the design of the program, to acquire communications of foreign targets with Americans as well as with others. And so as an inevitable result of that, millions of Americans' communications, which is the best estimate that anyone can have until the government provides a more accurate estimate, are being collected.

Mr. MARINO. Can you give me another example or an example of how you come to that conclusion?

Ms. GOITEIN. Sure. Well, one example is that there are 250 million Internet communications that are acquired each year under Section 702, at least that was the case in 2011. And this is collecting all of the communications of the targets. If you assume that——

Mr. MARINO. There's the big word, okay, "assume."

Ms. GOITEIN. Well, that's all we can——

Mr. MARINO. So are you basing this on a mathematical calculation?

Ms. GOITEIN. Unfortunately, after a year of asking for it, the intelligence community still has not given the Committee the numbers we would need to do an actual calculation. So if you conservatively assume that even 1 out of 100 of every foreign target's communications was with an American, that would still be millions of Americans' communications.

Mr. MARINO. You're dealing with a career prosecutor here. I don't assume anything.

Ms. GOITEIN. I would like not to assume. I would love to have the facts.

Mr. MARINO. Mr. Klein, what say you about that?

Mr. KLEIN. I actually agree with Ms. Goitein's description of incidental collection. I mean, this is something that has been documented by the Privacy and Civil Liberties Oversight Board, that this is a realistic prospect, that this happens in substantial volume.

And there have been statistical transparency reports by the intelligence community documenting, among other things, U.S. person identities that are part of disseminated intelligence reports. This is on page six of the 2016 transparency report.

So this is a real thing. But at the same time, there are measures in place to ensure that the U.S. person information collected through the program is minimized, is used only in specified ways subject to the supervision of the FISA court. So there are safeguards in place, but I do think that greater transparency would help boost public trust in that.

Mr. MARINO. And, Mr. Kosseff and Ms. Doss, do you have a thought?

Mr. KOSSEFF. I fully support transparency in terms of the numbers of incidental collections of U.S. persons' information. However, I also recognize there very well may be some logistical difficulties, as well as potential civil liberties concerns in terms of how you calculate and how you obtain that information.

I'm not an expert on that issue. I just know that's what's been stated in the public record. So I think that always will have to be balanced with the need for transparency. But absolutely, if there was a way to get those numbers, that would be excellent.

Mr. MARINO. Ms. Doss.

Ms. DOSS. From a practical perspective, I believe that it would be far more intrusive on privacy and really not feasible to come up with those numbers in a meaningful way, and I'll explain briefly why. I touched on it in my written testimony as well.

The challenge is that when the intelligence community is targeting a foreign intelligence target, there's no way a priori to know who the target will be in communication with. Intelligence analysts in their tradecraft typically look for communications of intelligence value, not for irrelevant ones, and when they see communications of value, they will inevitably find unknown identifiers, which might be phone numbers or email addresses.

The challenge is that there is nothing inherent in the unknown identifiers that can definitively point not only to where the other communicant might be, but to what their nationality and citizenship and identity are. So in order to make that determination, my view is the intelligence community would be required to have a significant amount of reference information about U.S. people who are of no intelligence interest in order to identify the U.S. person communications.

Ms. GOITEIN. Could I briefly respond to that?

Mr. MARINO. Briefly. My time has expired, but go ahead.

Ms. GOITEIN. Okay. For two of the programs under Section 702, it should be very straightforward to collect the information. For the phone collection, a country code will suffice as an estimate. There's no need to do research or have reference information. It's not 100 percent accurate, but it's accurate enough for the estimate that we seek.

For the purpose of Internet communications collected through upstream collection, the IP address serves as a proxy for country. It is a reliable enough proxy that the NSA relies on it to try to filter out domestic, wholly domestic communications. If it's reliable enough for that purpose, it's reliable enough for the estimate that we have sought.

The difficult program is PRISM. That's where it's a bit harder. And I would just say that we are aware of all of the problems in terms of trying to figure out the nationality of U.S. persons. There are privacy implications, but the privacy community has unanimously come down on the side of saying that it would be a net gain for privacy if there were a limited, one-time sampling under conditions that we have laid forward in a letter.

So while I appreciate Ms. Doss' concerns, I think the privacy community feels differently.

Mr. MARINO. My time has expired.

Congressman Lieu from California, you're up.

Mr. LIEU. Thank you, Mr. Chair.

Having served on Active Duty in the military, I believe when it comes to terrorists, we need to hunt them down and kill them. And I don't think anyone on this Committee has any problem with Section 702 and how it goes after foreign bad dudes and foreign Nations. I think some, and perhaps many of us, have a concern when we're talking about an American citizen and how they incidentally get caught up in this surveillance.

And under Section 702, if you're an American citizen and you're caught up in this surveillance, that information can be passed to the FBI to then do a criminal proceeding and do a criminal case against you. To me, that's just a flat-out violation of the Fourth Amendment.

And so for those of you who want a clean authorization, why do we even need that? Why don't we just require a warrant, as the Fourth Amendment does? How does going after American citizens for a criminal case that's unrelated to a target or foreign inquiry, how does that help our national security? And I guess that's my first question to those who think there should be no reforms to this section.

Mr. KOSSEFF. Well, to touch on that, one of the main justifications for having that ability has been that, let's say, that the FBI were searching for some—their unified database for an American U.S. identifier. They could then come up with a hit on 702 and that would tell them additional information about a potential foreign intelligence threat. So that's one justification.

And the other justification is going back to the wall between FBI and intelligence data that existed pre-September 11.

So those are two justifications for it. I also fully see your point on there being concerns about the FBI having that access.

When it comes to a Fourth Amendment issue, that's a little different. I'm not aware of any cases where a subsequent query of data that had been lawfully collected constitutes its own separate Fourth Amendment search.

So there very well may be some very strong policy reasons to change the FBI's ability to query that data, but I see that more as

a privacy and policy concern than a Fourth Amendment issue just under the doctrinal Fourth Amendment law.

Mr. LIEU. Thank you.

Yes, go ahead.

Ms. GOITEIN. I would disagree on the Fourth Amendment analysis. The notion that restrictions on searches of lawfully acquired information or lawfully accessed property is somehow not a part of the Fourth Amendment is simply not the case. It's actually the constitutional norm.

The terms of access to information or property are generally set forth in the warrant, and they usually do require limits on searches.

If I obtain a warrant to search a computer, for example, in a case where I have shown probable cause of a copyright infringement, I can take that computer, I can copy the hard drive, I lawfully have that information. But I am only permitted to search for the evidence of copyright infringement. After I find that, I can't go pulling up the IRS returns to look for evidence of tax fraud.

Uusually that's built into the warrant as a restriction on searching. It is part of the terms of access. The terms of access of 702, of getting this information without a warrant, is that the government has no intent to target any American, any particular known American. They have to certify our interest is only in the foreigner, not in any particular known Americans. And I would argue that that serves as a constitutional barrier to a warrantless search after collection.

Mr. LIEU. Thank you. And I think you had touched on this earlier. I just want to get it very clear from you. You would believe that responding to a request for information that this Committee has sent out to intelligence agencies about the statistics, you think that on balance it's better to get that information versus any privacy concern.

Ms. GOITEIN. Yes, I believe so, and 30 civil liberties organizations have signed a letter saying that, including the major national privacy organizations in this country.

Mr. LIEU. And let me conclude by just saying, you know, all of us here, and those intelligence agencies, took an oath not to an Administration or to a political party or to an agency, it was an oath to the Constitution.

And what that means is even if a program may be effective or not effective or incredibly brilliant, if it violates the Constitution, we just can't execute it unless we change the Constitution. And I just hope people understand that that's what it means when we all take an oath to the Constitution, that that is the primary document to which we owe our allegiance.

And with that, I yield back.

Mr. MARINO. The Chair recognizes the gentleman from Idaho, Mr. Labrador.

Mr. LABRADOR. Thank you, Mr. Chairman.

And thank you all for being here today.

I think it is the responsibility of this Committee and every Member of Congress to ensure that the privacy and the Fourth Amendment rights of every U.S. citizens are protected and remain of paramount importance to this government.

Professor Kosseff—am I pronouncing your name correctly?—in Ms. Goitein's testimony, she highlighted that, as of 2011, more than 250 million Internet transactions a year are being collected by the government. Is it possible to subject the collection of 250 million transactions a year to rigorous oversight?

Mr. KOSSEFF. Based on the procedures that the NSA has developed and my understanding of the procedures through the Privacy and Civil Liberties Oversight Board's report of it, I am very impressed by the multiple levels of analysis that have to go through, the targeting decisions, the certifications, and the minimization procedures, and the oversight for each, throughout all three branches of government.

So I do think that it is possible. I do think the volume, obviously, makes it very difficult. But I also don't think that's a reason not to do it. If there are ways to strengthen the oversight, then that would definitely be something worth looking at. But at least from a Fourth Amendment perspective, I think that is possible.

Mr. LABRADOR. Ms. Goitein, do you think it is possible to subject this to rigorous oversight?

Ms. GOITEIN. I think there is some indication, even in Ms. Doss' testimony, that it may be a little too much of a challenge, that while there has been no international lack of compliance with the rules, there have been repeated instances of noncompliance with FISA court orders and with court-ordered procedures.

I'm not talking about trivial technical violations. I'm talking about violations that were systemic, sometimes quite prolonged, and that resulted in significant overcollection and unauthorized searches.

Again, this was not through bad faith. There's essentially two explanations, and one is that the oversight isn't enough or isn't working, and the second explanation is that the system is so large and so technically and legally complex that compliance is effectively impossible.

Mr. LABRADOR. Well, let me just stop you there, because I only have 5 minutes.

So, for me, a particular concern—and this is not a political question. It just had a chilling effect on me, because I've been a critic of—or at least a proponent of strong reforms in this system now for several years. But I was concerned when I saw that Michael Flynn's information was made public.

So we have heard that there's supposed to be all these guidelines that are supposed to protect the identity of people. And whatever your political persuasion is, for me it had a chilling effect, that I thought my political opponents could use my personal information that they maybe gathered in some private communication against me in the future. So that should be quite terrifying to anybody, whether you're a Republican or a Democrat.

Mr. Kosseff, you mention that the numerous statutory limitations have been put in place to limit the invasion of privacy. It seems that, even with these limitations to protect the privacy of the average Americans, somehow leaks are happening. In Mr. Flynn's case, these leaks not only invaded his privacy but also crippled and ultimately prevented the Commander in Chief from having his key

national security personnel from doing its job, which you may have a political opinion about or not.

How do we trust these intelligence agencies to ensure that our national security when they're divulging highly sensitive information to settle scores or—can we prevent them from using this personal information to settle scores?

Mr. KOSSEFF. Well, I can't speak to those specific——

Mr. LABRADOR. So let's use that as an example, because that's an example that now the American people can relate to. It's what some of us have been warning about for years, and all of a sudden it happened, and it's a real-life example, where somebody's sensitive information was used for a political purpose, whether you agree with that political purpose or not.

Mr. KOSSEFF. Sure. So, putting that aside, I think in terms of the oversight, I think trust is by far the most important characteristic of a program like 702 or really any other intelligence program and——

Mr. LABRADOR. Well, but the Fourth Amendment was put in place because we don't trust the government.

Mr. KOSSEFF. Yes, yes.

Mr. LABRADOR. Ms. Goitein, without taking a political position on this, shouldn't we be alarmed by this?

Ms. GOITEIN. I think what you're touching on relates to essentially the history of FISA and why it was put in place, which is that surveillance was—and I'm not taking a position on the particular surveillance in this case. I'm taking a position more on your response to it and your sense that you're chilled, to some degree——

Mr. LABRADOR. Yes.

Ms. GOITEIN [continuing]. By the possibility that your communications could be acquired. And they could be. Under section 702, they could be.

And I think that is something that really ought to be of concern, because the statute is not narrow enough. It doesn't limit the government to conducting surveillance of foreign threats to the U.S. And that opens the door to potential abuses; it opens the door to possible political surveillance. That's why FISA was enacted in the first place in 1978, because those things were happening.

And section 702, while it responded to a real threat and it intended to address that threat in an effective way, it also eliminated some of the protections that might prevent the chilling that you're experiencing.

Mr. LABRADOR. Thank you.

Mr. MARINO. The gentleman's time has expired.

The Chair now recognizes the gentleman from Ohio, Mr. Jordan.

Mr. JORDAN. Thank you, Mr. Chairman.

Ms. Goitein, we sent a letter a year ago—your group may have been part of putting this letter together; I signed on to it—asking Mr. Clapper the number of Americans whose communications have incidentally been collected under section 702 of FISA.

Can you hazard a guess? They wouldn't give us a number. Can you hazard a guess?

Ms. GOITEIN. I had said earlier millions, which I think is conservative.

Mr. JORDAN. You think it's millions?

Ms. GOITEIN. Yes. Potentially tens of millions. I don't know. I really hesitate to speculate. I know that that speculation is discouraged. I wish I had better numbers for you.

Mr. JORDAN. So the response they give back to me—you know, they give a short, little three-paragraph response. And they say this—the operative sentence or clause says, "The numbers of Americans whose communications have been incidentally collected under 702 is a very difficult, if not an impossible, number to calculate."

That seems like baloney to me. It seems like that would be relatively easy to calculate. We're talking about the greatest intelligence service on the planet. You'd think they would be able to know that, right?

Ms. GOITEIN. Well, I think if we were asking for an accurate calculation, it actually would be difficult. We're asking for an estimate.

Mr. JORDAN. Right, an estimate.

Ms. GOITEIN. Certainly for two of the three programs under section 702, it should be quite straightforward.

Mr. JORDAN. Okay.

I just want to make sure I know exactly how this works. So there's a bad guy who's not an American, who's overseas, we want to surveil him. And this individual's going to communicate with an American.

So, on the front end, my understanding is the FISA Court says the procedures on how you're going to handle communications to and from or about Americans. On the front end, the FISA Court says, okay, those procedures, when you get in the situation, this is how you're going to conduct yourself. Is that right?

Ms. GOITEIN. Yes.

Mr. JORDAN. Okay.

And so now it happens; the bad guy communicates with an American. And we now have the American's phone conversation, the content of those phone conversations and the content of those email or whatever electronic communications, right?

Ms. GOITEIN. Yes. Presumably.

Mr. JORDAN. Okay.

And what happens when they look at—first of all, how are those communications stored?

Ms. GOITEIN. It depends on the agency. Let's say the NSA collects the communications.

Mr. JORDAN. Right.

Ms. GOITEIN. The NSA, through, let's say, the PRISM program. Then the NSA can just keep it in its own databases, can also give it to the FBI and to the CIA, the raw data with the American's information in it, to those agencies——

Mr. JORDAN. When you say "raw data," is that the content of the—the actual email content——

Ms. GOITEIN. Yes.

Mr. JORDAN [continuing]. And the actual content of those conversations?

Ms. GOITEIN. Yes.

Mr. JORDAN. Okay. So that that content could be on multiple databases.

Ms. GOITEIN. Correct.

Mr. JORDAN. FBI, NSA, various Federal agencies, right?

Ms. GOITEIN. Correct.

Mr. JORDAN. Okay.

Then how is it—then we have the term "query." What's that mean?

Ms. GOITEIN. A query is when an agent who is authorized to access the system and to run the query usually takes an email address or a phone number or some kind of identifier, a communications identifier, to search through the data for a particular individual's communications so that they can look at it.

Mr. JORDAN. Okay.

So we have it all there, and then they—let's say Joe Smith's the American. They have all the information on Joe Smith, and they said, now we want to query that. And it can be triggered just by the name? It could be triggered by what?

Ms. GOITEIN. I think it would be much more likely to be a phone number or an email address. That would be the way, I think, it's usually done.

Mr. JORDAN. Okay.

Ms. GOITEIN. I should say that the NSA and the CIA and the FBI all have rules that provide some limit on when they can query using a U.S. person identifier.

Mr. JORDAN. Is the information that was collected under a 702 about Americans, is it tagged differently in the databases that it's in, or is it just part of the overall database?

Ms. GOITEIN. It's tagged differently.

Mr. JORDAN. Tagged differently. So you could selectively go through and just say, I want information collected only under 702 about Americans?

Ms. GOITEIN. No. I think it would be more likely, actually, to work the other way, that whoever's running the query, if they get back information that's tagged as 702, they have to be trained in 702 in order to then access that information. But if they're not trained, they just go and ask someone else who is, and they come look at it.

Mr. JORDAN. Okay.

When they have that information about the American, can they use that information to—let's say the American's done something wrong. Could that American be prosecuted by information gained under 702?

Ms. GOITEIN. By the FBI, yes.

Mr. JORDAN. And could they be prosecuted only for crimes or potential crimes relative to national security, or is it broader than that?

Ms. GOITEIN. No. It's broader than that. It includes crimes that have no relationship to foreign intelligence or national security.

Mr. JORDAN. And has that happened?

Ms. GOITEIN. That information is not public.

Mr. JORDAN. Yeah. We don't know.

Ms. GOITEIN. And we would know if the government were more faithfully adhering to the notification requirements of the statute, under which the government is supposed to notify defendants when it uses information derived from section 702.

Mr. JORDAN. But do you think it has happened, where someone, an American, information gathered under 702 about that American is used to prosecute them and that's used to prosecute them in some area outside of national security? Do you think that has happened?

Ms. GOITEIN. I'm really not in a position to say. I don't know.

Mr. JORDAN. But can you hazard a guess?

Ms. GOITEIN. I'm sorry.

Mr. JORDAN. Do you think it's happened?

Ms. GOITEIN. Section 702 has certainly been used in criminal prosecutions that have a terrorism component, such as material support for terrorism. As for whether it's been used in a case that has nothing to do with national security, I'll put it this way: The FBI, according to the Privacy and Civil Liberties Oversight Board, routinely searches the data, data that includes section 702 data, for Americans' information when it's conducting criminal investigations that have nothing to do with national security. So I would imagine that, if they found something responsive, yes, they would use it. But——

Mr. JORDAN. Which is——

Ms. GOITEIN [continuing]. That is all I can say, really.

Mr. JORDAN. Yeah, which is scary.

Okay. I thank the Chairman, and I thank the witnesses.

Mr. MARINO. Before I go to Mr. Lieu, Ms. Doss, can you give us a little explanation concerning your experience about how tagging takes place, when something's tagged, if it's tagged, does a U.S. citizen's name comes up when this tagging takes place overseas?

Ms. DOSS. Thank you. Ms. Goitein's testimony fundamentally misstates the facts in that regard, so thank you for the opportunity to clarify.

The central challenge with identifying U.S. person communications in collected 702 data is that, by and large, the intelligence community will not have reference information to know who the U.S. persons are. They're targeting foreign persons for foreign intelligence reasons. The foreign intelligence target will communicate with any number of people, but, appropriately, the government does not have a comprehensive database of all of the identifiers, the phone numbers and email addresses, associated with the U.S. people.

So what happens is the data gets queried, looking specifically for foreign intelligence. When an unknown identifier is revealed, if there appears to be intelligence value in the communication, the analyst will then go do the due diligence research that will help them understand whatever information might be available about the communicant's nationality, location, identity. But there's no reference database that says, here's the U.S. people.

There are capacities within some—I can't speak for all of the databases that might hold 702 information everywhere in the CIA, FBI, and NSA. There are capacities to tag data as U.S.-person-related when it's recognized, but that requires recognition of it. There isn't any means, certainly not that I'm familiar with, that allows tagging of it upon arrival.

And one of the things that's really critically important that Ms. Goitein sort of slipped past in her previous testimony was that

there's two dimensions to this: location in the U.S. and U.S. people anywhere in the world.

For the question of whether somebody is located in the U.S., there are instances in which technical data can be helpful in making that determination, and it's critically important. It's not available for all types of 702 data, but it is for some, and that's critically important. That tells you location. That cannot tell you whether or not somebody might be a U.S. person anywhere else in the world, which, of course, is one of the key protections of 702.

Mr. MARINO. Mr. Lieu?

Mr. LIEU. Thank you, Mr. Chair.

So let me follow up on the gentleman from Ohio's question to you, Ms. Goitein. And you can also respond to what Ms. Doss said as well.

So let's say an intelligence agency is targeting a foreign national or foreign country, and then they find out incidentally that an American citizen is buying marijuana across State lines. Could that information be given to the FBI to then go prosecute that American citizen?

Ms. GOITEIN. Yes.

Mr. LIEU. How is that constitutional? I don't understand why your Fourth Amendment rights somehow get violated just because of how the information got collected on you, through this means. I don't understand that.

Ms. GOITEIN. I think if the government happens upon information of a crime that there is an argument that that's analogous to the "plain view" exception to the warrant requirement. Now, I think that that looks very different in a situation where you have a collection program that enables essentially the mass collection of hundreds of millions of communications a year. So I do think that's troubling. I'm much more troubled by the deliberate searching, which is not analogous to "plain view," for Americans' information.

And I do need to say that I did not say that Americans' information is somehow tagged as Americans' information. I believe I was asked the question whether section 702 data is tagged as 702 data. It's required to be tagged as 702 data in the statute.

So I think you misunderstood my testimony——

Ms. DOSS. My apologies if I misunderstood.

Ms. GOITEIN. Okay.

Mr. LIEU. Thank you.

So let me follow up on what you said, in terms of the scale of this program. So, under section 702, there's three categories, generally, in which intelligence agencies can go target. The first two I understand. One is terrorism. The second is, you know, nuclear nonproliferation issues and so on.

But the third is this massive category known as foreign affairs. So that could apply to academic students, human rights activists, lawyers. It's this massive group. And do you have any idea of how big that group is? Because foreign affairs is virtually everything, potentially.

Ms. GOITEIN. Again, we unfortunately have very, very little information about how that works in practice. Certainly it is a fear that under the very broad definition of "foreign intelligence information" in the statute, that would, on its face, encompass conversations of

human rights activists, conversations of journalists with their sources, NGOs that work on important political issues, and things of that nature.

One of the certifications on foreign intelligence topics was leaked, and that was the certification for foreign intelligence related to foreign powers. And the foreign powers about which the NSA is authorized to collect information that relates to those foreign powers includes most of the countries in the world, including allies of ours, including tiny countries that have very little role on the world stage, neutral countries with no history of terrorism. St. Lucia is on that list.

So certainly on paper these authorities are extremely broad. And we are trusting in the self-restraint of the people who are operating these programs to not take advantage of that breadth.

Mr. LIEU. Thank you.

And then one last question on the Fourth Amendment. As you know, the Fourth Amendment doesn't just say government can't engage in warrantless searches. It also says government can't engage in warrantless seizures.

So why isn't it the case that the seizure of an American citizen's email—that is a constitutional violation right there, before you even start searching. I mean, why is it the case that we even allow incidental collection of Americans? Why not just say, if there's incidental collection of Americans, we mask it, we delete it unless there's a warrant? Why wouldn't that be the case under the Constitution?

Ms. GOITEIN. Certainly one thing that I believe is constitutionally necessary—now, as I said, I think the courts have been applying some very old caselaw to come to different conclusions, but we need much, much stricter minimization requirements.

The minimization requirements that exist right now, which are described as strict, allow the NSA, the CIA, the FBI to hold on to Americans' data literally for years. If the FBI reviews data, sees Americans' data, comes to no conclusion about whether or not it is foreign intelligence, the 5-year limitation evaporates and they can hold on to it for some longer period that is still classified.

If the information's believed to contain secret meaning, which I think covers every email I ever sent to my sister, then that also is exempt from the age-off requirement.

Let's see, what else? The NSA is supposed to purge U.S. person data on detection if it doesn't contain foreign intelligence or evidence of a crime. The Privacy and Civil Liberties Oversight Board reported that this rarely, if ever, happens. The CIA and the FBI have no such requirement. They just rely on these very porous age-off requirements.

And all three agencies can search the data using U.S. person identifiers.

So if you look at these restrictions, such as they are, yes, there are restrictions on the use and retention of U.S. person data. But is that use and retention minimized? Not by any common sense of that word.

Mr. LIEU. Thank you.

I yield back.

Mr. MARINO. The Chair now recognizes the gentleman from Texas, Congressman Poe.

Mr. POE. Thank you, Chairman.

Thank you all for being here.

I'm going to pick up where my colleague just, I think, left off. And I want to keep it real simple for me—not for you, but for me.

The government, under secret courts, gets a secret warrant to seize information from a bad guy. Let's just call him "terrorist outlaw." And they grab that information from terrorist outlaw from their secret court, with secret information. And the warrant for that document, if you want to call it a warrant, is never publicized to the public.

Is that correct, Professor?

Oh, I guess when I say "professor," everybody looks at each other. I'll ask the witness that was just talking.

Is it "Goitein"?

Ms. GOITEIN. Goitein.

Mr. POE. Goitein. I apologize.

Is that correct? That document, we call it a warrant; I don't think it's a warrant. But that document is never made public. Is that correct? And that's part of FISA, that it's never made public.

Ms. GOITEIN. Correct.

Mr. POE. Okay.

So they seize information about outlaw terrorist, and in that information, they inadvertently come across data—emails, phone conversations—about some American. And they call that query. Is that correct?

Ms. GOITEIN. Not if they just stumble upon it. If they're looking for it, then that would be called a query.

Mr. POE. Okay.

Ms. GOITEIN. It's very technical. There are——

Mr. POE. I know.

Ms. GOITEIN [continuing]. Different ways they can find the information.

Mr. POE. But they seize it, is the point. They seize the information if they come across it, whether they're not looking for the information because the American's not the target. If it was the target, oh, my goodness, we'd have to get a search warrant. So they're going to say that he's not a target, or the American is not a target; they just come across the information, even inadvertently. And if it's on purpose, they've got to get a warrant, so I'm going to say it's inadvertently. Let's just assume, in my hypothetical, they come across it inadvertently.

And they read the information, or they have their computers read the information. And they seize that information, and they keep that information on whether it's one American or a bunch of Americans. Is that correct? I'm just asking.

Ms. GOITEIN. Yes.

Mr. POE. So they got that information——

Ms. GOITEIN. Seize it all together.

Mr. POE. Yeah, it's all together.

And they got that information. And I think what you said from the last question was they, in essence, keep that information forever.

Ms. GOITEIN. Not forever. Five years is the standard——

Mr. POE. But they've got excuses.

Ms. GOITEIN. But there are a lot of exceptions.

Mr. POE. A lot of exceptions, yeah.

So they've got this information. And I don't believe the NSA ever destroys information, ever, on anybody. But once they have that information—and then they determine that that information is that this person, this American, may have violated the law.

Then they make that person a target, they've got more information, and then they can file criminal charges on that information. Is that right or not?

Ms. GOITEIN. Well, I mean, what worries me is—I guess it depends what you meant by making the American a target. If they actually made the American a target, legally speaking, and went and got a warrant or a FISA Court order, we'd be in a different world. But that's not what happens.

Mr. POE. But that's not what they do. That's not what they do. They get the information, they read the information, it's inadvertent, "Oh, this guy may be a troublemaker as well," and they get more information based upon connecting all the dots to his emails, his phone calls, you know, his conversations with his mother-in-law. They get all that information, and then they can file criminal charges on him.

Ms. GOITEIN. That's right. And they don't just have to stumble upon the information. That's what the backdoor search is.

Mr. POE. Right.

Ms. GOITEIN. The backdoor search is when the FBI says: I have a criminal investigation on Joe Blow. And, look, I have this huge database. There's a bunch of section 702 data in it. But I'm going to query that data to see what I know about Joe Blow.

Mr. POE. That's right.

So they come across the information through a FISA warrant. They get the information on the American. And then they file criminal charges. And all of that is done without a search warrant under the Fourth Amendment to the Constitution of the United States against that American citizen, correct?

Ms. GOITEIN. That's correct.

Mr. POE. And I think that is illegal and a violation of the Constitution and an abuse of power by our government on Americans, for whatever my opinion is worth.

Mr. JORDAN. Mr. Chairman?

Mr. POE. I yield back.

Mr. MARINO. Mr. Jordan.

Mr. JORDAN. If I could, Mr. Chairman.

So, just the example that Judge Poe just went through, just to be clear, all the answers you gave when you get to that same individual, that individual could be prosecuted for you believe, something that's not related to national security as well.

Ms. GOITEIN. Well, I know that that individual can be prosecuted for something that's not related to national security. You had also asked whether I think that's actually happening. I think the FBI uses all the authorities it has.

Mr. JORDAN. Can I also ask, Mr. Chairman, how many times has the FBI—do we know how many times the FBI goes into that data-

base and actually uses information gathered either under the FISA example that the judge just described or under a 702 example that I described in my previous round of questions? Do you know how many times that happens?

We'll let the FBI answer. How about that?

Mr. KLEIN. The Privacy and Civil Liberties Oversight Board has commented on that, and they said that it's extremely rare that a query in a non-national-security investigation returns information about a U.S. person from 702, but we don't know what the exact number is. Actually, the FBI has been ordered by the Foreign Intelligence Surveillance Court to count that number.

So one pragmatic, relatively simple thing the Committee could do is require that number to be published, obviously not the details of the individual cases, but that top-line number could add some transparency. And if the number turns out to be really low, that might relieve some people's concerns about this practice.

Mr. JORDAN. Do you know that number, or you're currently trying to ascertain that number?

Mr. KLEIN. No, no, I don't, but the FBI does, because it has to report every case where a query in a non-national-security investigation comes back with 702——

Mr. JORDAN. Okay, then you misunderstood. The FBI knows that number right now.

Mr. KLEIN. They're counting every case, so they know the number. And they're reporting it to the Foreign——

Mr. JORDAN. But you're not allowed to give it to us today.

Mr. KLEIN. No. I'm a private citizen at a think tank, so I——

Mr. JORDAN. I thought you were with the FBI. Excuse me. I hadn't looked at the witness list that close. I thought you had some affiliation with the FBI.

Mr. KLEIN. Maybe I look like it.

Mr. JORDAN. You look like it.

Ms. GOITEIN. Could I add one quick thing to that? Which is I think it's also important, even though the court did not ask for this, for the FBI to report the number of——

Mr. MARINO. Okay. I have to ask you to just cease for a moment. The Chairman of the full Committee, Chairman Goodlatte, has to leave after he asks his questions, so then perhaps we can get back.

So the Chair recognizes Chairman Goodlatte.

Mr. GOODLATTE. Thank you, Mr. Chairman. And I have no problem with going back to Mr. Jordan's questions if he'd like to pursue them further.

And I do agree that we do need to address that issue with regard to what Fourth Amendment protections are given to U.S. citizens whose data goes through this process where it's taken by the NSA, a portion of that, a small portion, goes to the FBI, and the FBI saves it over a long period of time. I have questions both about the long-term retention of it and about what kind of threshold the government has to meet before they can use that information in a criminal case. So I think that's a legitimate issue that we need to consider as we reauthorize this program.

I also think it's very important that we reauthorize the program, however. And I want to turn back to Ms. Doss, so maybe you can get us focused on the positive value of this. Because it doesn't ap-

pear well-understood that the NSA is a Department of Defense entity that supports the warfighter. And as former counsel to the NSA, I'm sure you are more familiar than the rest of us that NSA intelligence supports our military.

So is 702 collection used to assist our men and women in uniform?

Ms. DOSS. In my experience, yes, absolutely, it is.

And former Director of the NSA Michael Hayden, when he was still there, talked often about the ways in which, in a post-9/11 world, tactical intelligence and national intelligence were really converging. Once upon a time, tactical intelligence to support warfighters on the battlefield was very much about troop movements.

It still, of course, includes that, but in an era of asymmetric terrorist activity and asymmetric warfare, as many of our troops overseas are engaged in, the same information about terrorist plans and intentions that can protect the national borders and the broader national security absolutely has proven critical to protecting the warfighter as well.

Mr. GOODLATTE. Thank you.

And, Mr. Klein, I appreciated your comments a moment ago. I'd like to follow up on the discussion about the Privacy and Civil Liberties Oversight Board, popularly known as PCLOB. And I'd like to know whether you believe that the PCLOB still serves as a valuable independent body for reviewing U.S. Government surveillance programs.

Mr. KLEIN. I do. I think it does.

Unfortunately, with only two members and soon to have one member, because one of the remaining members has been nominated for a high-ranking position in the Department of Justice, they do not have a quorum, which means they can't take official action. So, unfortunately, the Board is effectively paralyzed.

Mr. GOODLATTE. How many members of the Board are there?

Mr. KLEIN. There are five.

Mr. GOODLATTE. And how long has it been that there have been fewer than three?

Mr. KLEIN. It's relatively recent. The Chairman resigned last summer, which created its own problems. Only the Chairman can hire staff under the statute.

Mr. GOODLATTE. So is this an indication of a lack of interest or support in it by first the Obama administration, now the Trump administration? Or is it just circumstance that makes it ineffective right now?

Mr. KLEIN. I don't think it's specific to any Administration. This is a longstanding problem going back to when the Board was created. This is back well before 2010, and the Board scuffled around for years struggling to find enough members and staff to do its work.

I want to emphasize that this isn't just a privacy and civil liberties issue, although it is that. It's also an important issue for our national security. This is an important part of our case domestically but also to the international community that we have rigorous and multilayered oversight.

And evidence of that is the fact that the general counsel of the Office of the Director of National Intelligence in his letter explaining all of the rigorous oversight we have to our allies in Europe cited the Board as one element of that oversight.

So I think even if you support this program, as I do, if you think it's important for national security, if you want it to be perceived as credible, we need to keep this board going.

Mr. GOODLATTE. Should the reauthorization of the FISA Amendments Act look to strengthen the PCLOB?

Mr. KLEIN. Yes, I think it should. I actually have three specific proposals that the Committee can consider.

The most forward-leaning one is to require, as part of the FISA Court's annual review, it to certify that the President has made nominations to fill any vacancies. Now, I think it should be limited to nominations. We don't want this program getting caught up in nomination politics. But that would give Presidents an adequate incentive to staff something that, after all, doesn't report to the President; you can understand why it's not the number-one priority.

Mr. GOODLATTE. Are these Senate-confirmed?

Mr. KLEIN. These are Senate-confirmed positions. Four of them are part-time, but they're all Senate-confirmed.

Two other things that the Congress could do: The Board is subject to what's called the Government in the Sunshine Act. This applies broadly across the government to multimember agencies. But it's a very bad fit for this board, which, after all, does not exercise regulatory power. We're not talking about smoke-filled rooms and dealmaking here. This is just oversight. And four of them are part-time, so they need to collaborate informally. So requiring them to go through a very formal process just to hold a meeting really hampers them, unfortunately.

Mr. GOODLATTE. All right. We'll look at that. That's a good suggestion.

You had a third one as well?

Mr. KLEIN. Yes, I did. The Chairman is the only person who can hire staff. So if the Chairman resigns or is otherwise incapacitated, the Board is paralyzed from hiring staff.

Now, that's not an immediate problem right now, as I understand it; they are pretty well staffed up. But the Senate Intelligence Committee has proposed this, and I think it's a good idea: If the Chair is vacant, allow the other members to unanimously exercise the powers of the Chairman.

Mr. GOODLATTE. Thank you.

Professor Kosseff, can privacy and national security coexist?

Mr. KOSSEFF. Absolutely. And I think 702 is a good example of it, in terms of the various levels of oversight from all three branches of the government, the development of minimization and targeting procedures, both by the executive branch and being approved by the FISA Court. I think that that shows a real concern for both protecting national security while making sure that privacy still is at the forefront.

Obviously, all of the procedures can be improved. And, on the flip side, there's never going to be perfect security or perfect privacy, and there's always going to be some policy decisions to be made.

But I do think 702, in many ways, is a model of considering both the very difficult considerations of security in an era when our telecommunications infrastructure is very different from the 1978 era, when we initially had FISA, while at the same time protecting privacy.

So the answer is, yes, absolutely.

Mr. GOODLATTE. Some have argued that section 702 must respect human rights, essentially extending American constitutional rights to foreign nationals. Do you have an opinion on extending constitutional rights to foreigners?

Mr. KOSSEFF. I think that's a tough decision—or a tough issue that's come up with the ICCPR issue as well as PPD-28. And I think, in some ways, there are a number of statutory provisions within 702 that do apply both to U.S. persons and non-U.S. persons, including the various disclosure limits, the purpose limits, penalties for misuse. So I'd be concerned about extending, just as a practical matter of government surveillance and intelligence operations, and I think on the——

Mr. GOODLATTE. It would completely change the meaning——

Mr. KOSSEFF. Yeah, yeah.

Mr. GOODLATTE [continuing]. Of intelligence gathering, wouldn't it?

Mr. KOSSEFF. Yeah.

Mr. GOODLATTE. It would put the U.S. at a severe disadvantage, since I'm not aware of other major countries that gather intelligence respecting even the rights of their own citizens, much less foreign nationals.

Mr. KOSSEFF. I think it's a tough balance. I think there's a lot of concern about if the United States is not seen as adequately respecting privacy of non-U.S. persons, then there could be implications for the privacy shield, for example.

But I don't have personal experience in intelligence operations, but I think it would probably create a number of very difficult logistical issues if we were to do that.

Mr. GOODLATTE. Very good. Thank you.

Thank you, Mr. Chairman. And, Mr. Chairman, if you wouldn't mind, after you've asked the additional questions you wish to, just adjourn the hearing.

Mr. JORDAN [presiding]. Yep. I'd be happy to. Thank you.

Mr. GOODLATTE. Thank you.

Mr. JORDAN. I want to thank the Chairman for his questions and work.

The Chairman asked the question, can privacy and security coexist, but—and I have utmost respect for the Chairman, but it seems to me the question for this Committee is not that question. The question for this Committee, the question for all of us is, is 702 consistent with the Constitution. I mean, that's the fundamental question.

And, Mr. Kosseff, do you think that that's, I guess, the appropriate question, and do you think it's actually happening?

Mr. KOSSEFF. I think it is the appropriate question. And I think, based on what we have in the public record of how 702 operates, I think that it currently is consistent with the Fourth Amendment, but I give two important caveats.

First, it's not a static answer. The answer could always change in the future based on any additional discovery of operational problems with 702 or how it's being used. And I think one key to that is figuring out exactly how you analyze the Fourth Amendment issues.

Mr. JORDAN. Yes.

Mr. KOSSEFF. As I've testified early——

Mr. JORDAN. I guess you think it's constitutional, but it sounds like you think it's pretty darn important to be skeptical——

Mr. KOSSEFF. Absolutely.

Mr. JORDAN [continuing]. Or be concerned.

Mr. KOSSEFF. Absolutely.

Mr. JORDAN. I would argue that too. I mean, think about what we've witnessed in last several years. We saw the IRS target people for exercising their First Amendment free speech rights, go after people for political reasons. I mean, you could look at the Flynn situation that Congressman Labrador brought up.

So, in that context, holy cow, I would almost say we better be more than skeptical, we better be cynical about it.

Keep going. I'm sorry.

Mr. KOSSEFF. I think there needs to be constant, rigorous oversight. I think that there has been, both from your Committee, the other Committees, as well as the FISA Court, if you look at some of the changes that have been made to things like the MCT issue in response to the FISA Court. I think there has been rigorous oversight. But I think it has to be constant. And we can't just rest on one assessment that it's operating fine; it has to be constantly evaluated.

Mr. JORDAN. Okay.

Ms. Doss, do you think that's the appropriate question, is 702 consistent with the Constitution?

Ms. DOSS. Absolutely. And, in my view, it is——

Mr. JORDAN. Okay.

Ms. DOSS [continuing]. Both as——

Mr. JORDAN. I had a feeling you were going to say that. Yeah, yeah.

And, Ms. Goitein, what do you think?

Ms. GOITEIN. I certainly think it's the most important question. In my view, it's not constitutional, but I don't dispute the authority of the judges who have said otherwise. I just think that, as I said, this is a case of the law failing to keep up with technology. That happens. That happens often. And it becomes your job to step in and fill the constitutional gap.

Mr. JORDAN. Mr. Klein?

Mr. KLEIN. Yes, I agree that that's the first question. I don't think it's necessarily the last question. Even if it is constitutional, which I personally believe it is—and two courts have said so—you can ask whether it's wise or whether there's more information that we'd like to collect.

So, on the subject of incidental collection, which you talked about before, how much of Americans' data is getting caught up in this, the Privacy and Civil Liberties Oversight Board actually recommended five categories of data, including several of the things that Ms. Goitein was talking about, that the intelligence commu-

nity is supposed to collect and report to Congress and to publish, to the extent consistent with national security. That's called Recommendation 9.

Mr. JORDAN. Okay.

Mr. KLEIN. That's a good place to start. So there are things we can do inform——

Mr. JORDAN. Let me ask about that, the dialogue you had with the Chairman on this Civil Liberties Protection Board or whatever the official title is. I asked you questions my last round about how many times the FBI queries the database and they get information that was derived from a 702. Does this oversight board know that number?

Mr. KLEIN. Nobody knows the exact number of queries. The reason is that the FBI does not normally code its queries for nationality, because nationality is not relevant to most investigations. I think it would be good to have an estimate of the number of queries. It's a fairly routine practice, according to the Board, so the estimate would be high.

Mr. JORDAN. So, on the same question I started off—about a half an hour ago, I asked a question that we sent to Mr. Clapper about the number of communications or transactions involving United States persons subject to 702 surveillance on an annual basis, and we got the response back and said they couldn't figure that out. Does this board know that number?

Mr. KLEIN. They don't, no. Nobody knows that number. To do that, they would have to either go through every communication, which is simply infeasible, or some representative——

Mr. JORDAN. We just heard—I mean, I've got to believe that the NSA knows that number or they can get an estimate. Does the Board know the estimate?

Mr. KLEIN. No. There is no estimate.

I mean, the reason why an estimate might be difficult is because emails typically don't disclose, on their face, the nationality of the people communicating. In some cases, you might have the information telling you the location from where the email was sent; in other cases, you might not. Even still, that's not a perfect proxy.

And the question is, to find that out, to find out if the person is a U.S. citizen, what else would you have to do? Would you have to use other types of surveillance to get additional information about who that email address belongs to? That could create greater privacy harms.

So, while I agree with the motivations behind the letter and I agree that the estimate would be worth having and a good thing to have, I do sympathize with the intelligence community because there are real, practical obstacles that they're facing in creating such an estimate.

That's why I think we should look at the Recommendation 9 from the Privacy Board. There are five types of information that are a decent starting point for finding out incidental collection. Let's get those counts, let's get them public to the extent possible.

Mr. JORDAN. Tell me those five.

Mr. KLEIN. Let's see. I have them here.

Mr. JORDAN. Or have you given us something in writing on that already? Okay. That's fine.

Mr. KLEIN. Yeah, I mean, I can read them, but it'd probably be better to give them to you in writing.

Mr. JORDAN. That's fine. That's fine. All right.

Ms. Goitein?

Ms. GOITEIN. Quickly. The NSA has determined that the IP address is an accurate enough indicator of a person's status as a U.S. person being domestically located, or being located overseas, to use it to filter out the wholly domestic communications that the NSA is prohibited from acquiring.

If it's accurate enough to enable the NSA to comply with that constitutional obligation, then it's certainly accurate enough for the estimate——

Mr. JORDAN. It's certainly accurate enough to give us a count.

Ms. GOITEIN [continuing]. That we're looking for.

And just one other quick point about oversight and the importance of oversight, which I do not dispute; I think oversight is incredibly important. But it's not an end in itself, and it's never a substitute for adequate substantive limits in the law. If the law and the rules allow the FBI to read Americans' emails without obtaining a warrant, then the FBI could be scrupulously adhering to those rules and we still have a problem.

Mr. JORDAN. Yep. Well-said.

I want to thank you all for being here today.

And the Committee is adjourned.

[Whereupon, at 4:45 p.m., the Committee was adjourned.]

○